Toni Alho

JULKISTEN ORGANISAATIOIDEN KOLLABORAATIOTYÖKALUT JA VIRANOMAISVAATIMUSTEN TÄYTTÄMINEN SUOMESSA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2023

TIIVISTELMÄ

Alho, Toni
Julkisten organisaatioiden kollaboraatiotyökalut ja viranomaisvaatimusten täyttäminen Suomessa
Jyväskylä: Jyväskylän yliopisto, 2023, 48 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja: Seppänen, Ville

Kollaboraatiotyökalut ovat organisaatioiden modernin työnteon perusvälineitä. Nämä työkalut mahdollistavat tehokkaan kommunikaation ja yhteistyön niin organisaation sisällä, kuin myös ulkoisten henkilöiden tai muiden organisaatioiden välillä. Kollaboraatiotyökaluille ominaista on niiden toimittaminen julkipilvestä SaaS-mallilla, minkä vuoksi työkaluja hyödyntävien organisaatioiden on otettava huomioon myös pilvipalveluiden ominaisuudet työkalua valitessaan. Suomalaisen julkisen sektorin toimijoita koskee sekä Euroopan unionin että kansallisen tason lainsäädäntö ja viranomaisohjeistus. Tässä tutkimuksessa perehdyttiin tarkemmin suomalaisten julkisten organisaatioiden kollaboraatiotyökaluihin vaikuttavaan lainsäädäntöön sekä ohjeistukseen ja siten pyrittiin selvittämään mitä vaatimuksia kollaboraatiotyökalujen käyttämiseen liittyy. Käsitys siitä, mitä suomalaisten julkisten organisaatioiden on huomioitava käyttäessään tai hankkiessaan kollaboraatiotyökaluja, muodostettiin kirjallisuuskatsauksen avulla. Näiden havaintojen perusteella luotiin design-tutkimuksen keinoin suomalaisten julkisten organisaatioiden kollaboraatiotyökalun valitsemista ja sen vaatimustenmukaisuuden selvittämistä tukeva artefakti, eli tarkistuslista.

Asiasanat: kollaboraatiotyökalut, pilvipalvelut, julkiset organisaatiot, henkilötietojen käsittely

ABSTRACT

Alho, Toni
Collaboration tools of public organization and fulfilling the regulatory requirements in Finland
Jyväskylä: University of Jyväskylä, 2023, 48 pp.
Information Systems, Master's Thesis
Supervisor: Seppänen, Ville

Collaboration tools are essential for modern work in organizations. These tools enable efficient communication and collaboration both within the organization and with external individuals or other organizations. One characteristic of collaboration tools is that they are delivered from the public cloud using the SaaS delivery model, which is why organizations using these tools must also consider the features of cloud services when selecting a tool. Finnish public sector actors are subject to both European Union and national legislation and official guidelines. This study examined the legislation and guidelines that affect collaboration tools used by public organizations in Finland, with the aim of determining the requirements associated with using these tools. The understanding of what Finnish public organizations need to consider when using or acquiring collaboration tools was obtained through a literature review. Based on these observations, a design research artifact, a checklist, was created to support the selection and evaluation of collaboration tools for Finnish public organizations.

Keywords: collaboration tools, cloud computing, public organizations, personal data processing

KUVIOT

SISÄLLYS

1 JOHDANTO

Euroopan Unionin ja sen eri elinten työ henkilötietojen suojaamiseksi on ravistellut Euroopan ja Yhdysvaltain välisen datankulun ja erityisesti pilvipalvelumarkkinan kenttää. Yleinen tietosuoja-asetus (GDPR), Euroopan unionin tuomioistuimen Schrems -päätökset sekä ajatus eurooppalaisesta digitaalisesta suvereniteetista ovat luoneet eurooppalaisille ja siten myös suomalaisille toimijoille motivaatiota siirtää datansa eurooppalaisten palveluntarjoajien konesaleihin, taatakseen näin datan käsittelyn vaatimustenmukaisuuden. Tämä pro gradu -tutkielma pyrkii luomaan katsauksen suomalaisten julkisten organisaatioiden kollaboraatiotyökaluja koskevaan lainsäädäntöön ja viranomaisvaatimuksiin sekä tuottamaan tähän kenttään julkisia organisaatioita hyödyttävän tuotoksen.

1.1 Tietosuojan historia Euroopassa

Yhdysvaltalainen politiikan tutkija ja professori Abraham L. Newman on esittänyt fasistisen perinnön teorian, jonka mukaan eurooppalaisten historialliset kokemukset totalitarismista ja fasismista olisivat opettaneet Euroopan suojelemaan ja puolustamaan yksityisyyttään. Yksityisyyttä tutkineen Hannoverin yliopiston professori Wolfgang Kilianin mukaan varsinkin saksalaiset ovat tämän historiallisen painolastin myötä erityisen huolellisia kansalaisten yksityisyyden suojasta. Saksa onkin maailman ensimmäisiä tietosuojaa koskevaa lainsäädäntöä käyttöönottaneita valtioita. (Rossi, 2018)

Tämä kulttuurinen perintö on mahdollisesti myötävaikuttanut Euroopan unionin suhtautumiseen ja toimintaan henkilötietoja koskevassa lainsäädännössä (Politou ym., 2018). Ensimmäisen henkilötietojen suojelua koskevan direktiivin Euroopan unioni määräsi jo vuonna 1995, ja direktiivillä vaikutettiin nimenomaan automatisoituun tietojenkäsittelyyn. Kyseisellä direktiivillä pyrittiin rakentamaan oikeudellinen kehys, joka loisi tasapainon yksityisyyden suojan ja henkilötietojen vapaan liikkuvuuden välille. Tämä tietosuojadirektiivi sisälsi monia nykyhetken yksityisyydensuojaa koskevia säännöksiä ja periaatteita, kuten

rekisteröidyn oikeuden saada tutustua hänestä kerättyihin tietoihin sekä tietojen laatua ja käsittelyä koskevia periaatteita. (Euroopan parlamentti ja Euroopan unionin neuvosto, 1995)

Tietosuojadirektiivin mukaan henkilötietoja oli sallittua siirtää kolmansiin maihin vain, jos kyseisessä maassa turvataan riittävä tietosuojan taso – muutoin henkilötietojen siirto olisi kiellettävä. Tämän vaatimukset täyttämiseksi Euroopan unionin ja Yhdysvaltojen välillä otettiin vuonna 2000 Euroopan komission päätöksellä käyttöön Safe Harbor -periaatteet (Euroopan komissio, 2000). Näitä periaatteita noudattamalla henkilötietojen suojelun katsottiin olevan Yhdysvalloissa riittävää aina vuoteen 2015 saakka.

Samoin vuonna 2000 oikeus henkilötietojen suojaan esiteltiin myös Euroopan unionin perusoikeuskirjassa, kahdeksannessa artiklassa. Kyseisen artiklan mukaan henkilötietojen käsittelyn on oltava muun muassa asianmukaista, jokaisella on oltava oikeus tutustua itsestään kerättyihin tietoihin ja riippumattoman viranomaisen on valvottava sääntöjen toteutumista. (Euroopan parlamentti neuvosto ja komissio, 2000). Nämä perusoikeuskirjaan kirjatut oikeudet, erityisesti artiklat 7, 8 ja 46, ovat vaikuttaneet oleellisesti myöhempään tietosuojaa koskevaan lainsäädäntöön ja sen tulkintaan Euroopan unionissa.

2000-luvulla digitalisaatio otti harppauksia ja vuoden 1995 henkilötietoja koskeva direktiivi koettiin vanhentuneeksi 2010-luvun alkupuolella. Työ uuden tietosuojaa koskevan lainsäädännön luomiseksi pyrki korjaamaan vuoden 1995 direktiivin puutteita ja huomioimaan uusia yksityisyyden suojaa koskevia haasteita. Uusi lainsäädäntö tulisi myös olemaan kaikkia Euroopan jäsenmaita velvoittava asetus, aiemman kansallisia muokkauksia sallivan direktiivin sijaan. (Rossi, 2018)

Asetuksen valmistelu kohtasi merkittävää vastustusta erityisesti yksityiseltä sektorilta ja vuonna 2013 sen pelättiin vesittyvän täysin, pahimmillaan jopa heikentäen silloista henkilötietojen suojan tasoa (Rossi, 2018). Fiaskoksi ennakoidun lainsäädännön sisältöön ja toteutumiseen vaikuttanut käänne tapahtui kuitenkin kesäkuun 7. päivä, kun The Washington Post ja The Guardian julkaisivat Edward Snowdenin vuotamat dokumentit erityisesti Yhdysvaltain kansallisen turvallisuusvirasto NSA:n harjoittamasta maailmanlaajuisesta joukkovalvonnasta. Näiden Snowdenin paljastusten voidaan katsoa laittaneen liikkeelle uuden ajatuksen kansallisen ja Euroopan laajuisen digitaalisen suvereniteetin luomisesta (Pohle & Thiel, 2020), minkä myötä teknologinen ja digitaalinen itsenäisyys, sekä Euroopan kyvykkyys toimia itsenäisesti digitaalisessa maailmassa on tänä päivänä noussut yhdeksi Euroopan unionin tärkeimmistä kysymyksistä (Tambiama, 2020).

Snowdenin paljastukset muuttivat perusteellisesti vuoden 2013 tietosuojalainsäädäntöä koskevaa keskustelua, mikä johti sittemmin yleisenä tietosuoja-asetuksena (General Data Protection Regulation, GDPR) esitellyn asetuksen kehittämiseen. Paljastuneesta valvontajärjestelmästä raivostuneiden eurooppalaisten huomio Internetin yksityisyyden haasteita kohtaan moninkertaistui ja jo seuraavana vuonna Euroopan parlamentin täysistunto äänesti ennakoidun vastaisesti jopa maailmanlaajuisesti tunnustetun, vahvan tietosuoja-asetuksen

puolesta äänin 621 – 11 (Rossi, 2018). Tietosuoja-asetus astui lopulta voimaan huhtikuussa 2016 kumoten vuoden 1995 tietosuojadirektiivin ja sitä alettiin soveltaa toukokuussa 2018 (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016).

Samoihin aikoihin Snowdenin paljastusten kanssa itävaltalainen Maximillian Schrems teki Irlannin tietosuojavaltuutetulle valituksen koskien Facebookin tekemää henkilötietojen siirtoa Irlannista Yhdysvaltoihin. Schrems näki, että Facebook ei pystynyt Yhdysvalloissa takaamaan henkilötiedoille riittävää tietosuojaa, kuten vuoden 1995 tietosuojadirektiivissä edellytetään, ja vaati tietosuojavaltuutettua kieltämään Facebookia siirtämästä hänen henkilötietojaan Yhdysvaltoihin. Irlannin tietosuojavaltuutettu vetosi Safe Harbor -periaatteisiin ja kieltäytyi käsittelemästä valitusta. Tämän myötä Schrems vei asian Irlannin tuomioistuimeen, joka edelleen teki asiasta ennakkoratkaisupyynnön Euroopan unionin tuomioistuimeen. (Costello, 2020)

Tämä tapaus, joka nykyisin tunnetaan nimellä ”Schrems I”, päättyi Euroopan unionin tuomioistuimen vuonna 2015 antamaan tuomioon, jossa Safe Harbor -periaatteet todettiin riittämättömäksi ja niitä koskeva vuoden 2000 päätös siten pätemättömäksi. Tuomio perustui erityisesti vuoden 1995 tietosuojadirektiiviin ja Euroopan unionin perusoikeuskirjan artiklojen 7, 8 ja 47 sisältöön, eli perimmillään Euroopan unionin tunnustamiin perusoikeuksiin. Tuomiossa huomionarvoista oli myös Euroopan komission toteamus siitä, että kaikki Yhdysvaltain tiedustelupalvelun joukkovalvontaan osallistuneet yritykset (mm. Google, Facebook, Apple, Microsoft ja Yahoo) näyttivät kuuluvan Safe Harbor -järjestelmään, eikä näiden yritysten eurooppalaisten asiakkaiden perusoikeuksia voitu Safe Harbor -periaattein turvata. (Euroopan unionin tuomioistuin, 2015)

Yhdysvalloissa ja Euroopan unionissa alettiin hakea uutta ratkaisua transatlanttisen datan liikkuvuuden turvaamiseksi. Yhdysvalloissa esitettiin ajatuksia liittovaltion yksityisyydensuojaa ja valvontaa koskevan lainsäädännön kehittämisestä, mutta sen sijaan vuonna 2016 EU:n ja Yhdysvaltain välille neuvoteltiin uusi Safe Harborin kaltainen järjestely Privacy Shield. Privacy Shield sai välittömästi moitteita monilta oikeus- ja kuluttajaryhmiltä, eikä sen uskottu takaavan riittävää tietosuojaa Euroopan unionin kansalaisten henkilötiedoille. Vain kaksi vuotta myöhemmin Euroopan parlamentissa alettiin vaatia järjestelyn rajoittamista, erityisesti läntistä maailmaa ravisuttaneen Facebook – Cambridge Analytica -skandaalin paljastuttua. (Rotenberg, 2020)

Cambridge Analytican tapauksessa Facebookin käyttäjistä kerättyjä tietoja oli hyödynnetty vaalivaikuttamiseen niin Yhdysvalloissa (presidentinvaalit 2016) kuin Euroopassakin (Brexit -kansanäänestys 2016). Kumpikin yhtiö toimi tietojen keräämisen aikana Privacy Shield -järjestelyn alla. Paljastusten myötä Euroopan parlamentissa nostettiin esiin huoli henkilötietojen väärinkäytön synnyttämästä uhasta demokraattisia prosesseja kohtaan (Rotenberg, 2020).

Vuonna 2018 Irlannin tietosuojavaltuutettu pyysi Maximillian Schremsia muotoilemaan aiemman valituksensa Facebookin tietojen siirrosta Yhdysvaltoihin, tällä kertaa koskien Privacy Shield -järjestelyn liitteessä asetettuja, mutta jo aiemmin käyttöön otettuja mallisopimuslausekkeita (Standard Contractual

Clauses, SCC). Tämä kanne eteni jälleen Irlannin tuomioistuimen kautta Euroopan unionin tuomioistuimeen, missä tarkasteltiin Privacy Shieldin sekä mallisopimuslausekkeiden pätevyyttä. Tapaus tunnetaan nimellä Schrems II. (Costello, 2020)

Vaikka tapaukseen Schrems II johtanut valitus perustui jo kumottuun tietoturvadirektiiviin, valituksen tarkastelu ulotettiin EU:n tuomioistuimessa direktiivin korvanneeseen yleiseen tietosuoja-asetukseen (GDPR). Tuomiossa tarkasteltiin voimassa olevan lainsäädännön (GDPR:n) tulkintaa jälleen kerran EU:n perusoikeuskirjan artikloja 7, 8 ja 47 vasten. Tiivistäen, EU:n tuomioistuin totesi ettei Privacy Shield -järjestely täyttänyt EU:n perusoikeuskirjan mainittujen artiklojen ja yleisen tietosuoja-asetuksen vaatimuksia. Tässä vuoden 2020 päätöksessä Privacy Shield todettiin pätemättömäksi, mutta toisaalta mallisopimuslausekkeita koskeva päätös säilytettiin pätevänä. (Costello, 2020; Euroopan unionin tuomioistuin, 2020)

Schrems II -päätöksen jälkeen Euroopan komissio päivitti mallisopimuslausekkeet vastaamaan yleistä tietosuoja-asetusta sekä Schrems II -päätöstä. Nämä uudet lausekkeet, joita kutsutaan vakiolausekkeiksi, ovat Privacy Shieldin pätemättömäksi toteamisen jälkeen olleet ainoa tapa järjestää henkilötietojen siirto Yhdysvaltoihin. Niiden pätevyys ja valvonnan toteutus ovat kuitenkin aiheuttaneet runsaasti kysymyksiä niin tietoja siirtävissä organisaatioissa kuin muissakin toimijoissa.

Euroopan unioni, erityisesti unionin tuomioistuin, on siis tehnyt selväksi EU:n perusoikeuskirjan yksityisyyttä ja henkilötietojen suojaa käsittelevien perusoikeuksien merkityksen. Euroopan unioni on näiden tapahtumien myötä ottanut myös ajatuksen digitaalisesta suvereniteetista osaksi eurooppalaista kulttuuria edustavaa toimintaansa, mutta hakee edelleen keinoa Safe Harborin ja Privacy Shieldin kaltaisen järjestelyn toteuttamiselle. Tulevaisuuden suhteen on kuitenkin epäselvää, voiko näitä eurooppalaisia arvoja ja oikeuksia kunnioittavaa henkilötietojen siirtoa Yhdysvaltoihin toteuttaa ilman muutoksia Yhdysvaltain lainsäädäntöön.

1.2 Tutkielman tausta

Euroopan unionin henkilötietojen suojaa koskeva työ on luonut haasteita niin eurooppalaisten kuin yhdysvaltalaistenkin organisaatioiden toiminnalle globaalissa markkinassa. Epävakaa ja pahimmillaan tulkinnanvarainen lainsäädäntö sekä viranomaisohjeistus tekevät organisaatioiden informaatioteknologiaa ja dataa koskevista päätöksistä vaikeasti ennakoitavia ja epävarmoja. Monet eurooppalaiset organisaatiot ovat tunnistaneet myös henkilötietojen siirtoa koskevan ratkaisemattoman haasteen, Yhdysvaltain lainsäädännön, tuottamat lainsäädäntöjohdannaiset riskit henkilötietojen suojaamiselle.

Useat organisaatioiden laajassa ja päivittäisessä käytössä olevat ohjelmistot ja järjestelmät ovat suurten yhdysvaltalaisten yhtiöiden tuottamia ja tarjoamia. Eräitä tällaisia tuotteita ovat muun muassa Microsoftin Office / Microsoft 365 -

tuoteperhe, Googlen Workspace -palvelut ja nykyisin Salesforcen omistama Slack. Näitä tuotteita voidaan kuvailla kollaboraatiotyökaluiksi, ne mahdollistavat organisaation jäsenten sisäisen ja ulkoisenkin yhteistyön, helpottaen muun muassa tiedon jakamista ja etäkokousten järjestämistä. Ominaista näille kollaboraatiotyökaluille on niiden toteutus pilvipalveluiden palvelumallilla Software as a Service (SaaS), jossa kaikki asiakkaan tai käyttäjän tuottama, käsittelemä, tallentama tai siirtämä data kulkee ja varastoituu palveluntarjoajan palvelimilla. Jos kyseessä on yhdysvaltalainen palveluntarjoaja, palveluissa käsiteltyjen henkilötietojen tietoturvaa ja lainsäädäntöjohdannaisten riskien torjumista voi olla vaikea tai jopa mahdotonta varmistaa.

Henkilötietojen turvaamiseksi ja varmuudella myös tulevan lainsäädännön sekä viranomaisohjeistuksen noudattamiseksi organisaatioiden kiinnostus vaihtoehtoisia, ei-yhdysvaltalaisia palveluita kohtaan on kasvanut. Euroopan unionissa vahvistunut ja aktiivisesti edistetty ajatus digitaalisesta suvereniteetista luo myös eurooppalaisille organisaatioille painetta ja halua ”ottaa datansa omiin käsiinsä” (Pohle & Thiel, 2020; Tambiama, 2020). Laajimmin jokapäiväisessä käytössä olevat ohjelmistotuotteet, kuten Microsoft Office / 365, ovat kuitenkin saavuttaneet lähes de facto standardin aseman, eikä korvaavan vaihtoehdon valitseminen ole organisaatioille helppoa. Korvaavia vaihtoehtoja kuitenkin on olemassa.

Ruotsalainen julkisten organisaatioiden muodostama eSam-verkosto on julkisen sektorin kollaboraatioalustoja koskevassa raportissaan todennut, että Yhdysvaltoihin sidotuille palveluille on selkeästi olemassa vaihtoehtoja, osin jopa parempia kuin yleisessä käytössä olevat yhdysvaltalaiset palvelut. Raportissa painotetaan, että julkisilla organisaatioilla ei ole tarvetta ”navigoida laillisuuden harmaalla alueella täyttääkseen tarpeitaan”, eikä syytä ”kuluttaa aikaa ja resursseja tietojen suojaamiseen palveluntarjoajalta”. Raportti painottaa myös, että julkisella sektorilla on mahdollisuus näyttää esimerkkiä tietoturvallisten palveluiden käyttöönotossa ja kansalaisten henkilötietojen suojaamisessa. (Anderson ym., 2021).

eSamin raportin jälkeen Pohjoismaissa on tehty toimia kollaboraatiotyökalujen tietosuojan takaamiseksi. Ruotsissa Tukholman kaupunki on riittämättömän henkilötietojen suojan vuoksi kieltäytynyt ottamasta käyttöön käytännössä Microsoft Officesta koostuvaa Microsoftin 365 -tuoteperhettä. Lisäksi selvitys nosti esiin palvelun yksipuolisen toimituksen ja sopimuksen muuttamisen muodostamat riskit. (Malmqvist, 2022)

Tanskan tietosuojavaltuutettu Datatilsynet puolestaan on Helsingørin kunnan kouluja koskevan tapauksen myötä kieltänyt Google Chromebookien ja Workspace -palveluiden käytön Tanskan kouluissa (Datatilsynet, 2022). Suomen tietosuojavaltuutettu on myös ilmoittanut tekevänsä selvitystä julkisen sektorin pilvipalveluiden käytöstä yhdessä Euroopan tietosuojaneuvoston kanssa (Tietosuojavaltuutetun toimisto, 2022). Tämän selvityksen tuloksista ei kirjoitushetkellä ole vielä tietoa.

Näihin Ruotsin ja Tanskan päätöksiin johtavan EU-lainsäädännön vaikuttaessa samalla tavalla myös Suomessa, on odotettavaa että myös suomalaiset

julkiset organisaatiot joutuvat ainakin varautumaan Microsoftin ja Googlen kollaboraatiotyökalujen korvaamiseen. Ruotsin veroviranomainen on tehnyt pohjoismaisittain pioneerityötä laajan selvitystyön parissa nykyisten kollaboraatiotyökalujen korvaamiseksi, joskaan hankintoja ei ole vielä tehty. Suunta on kuitenkin selvä. Ruotsin veroviraston mukaan kollaboraatiotyökalujen jälkeen tarkasteltavana ovat myös HR-järjestelmät, mahdollisten tulevienkaan lainsäädännön muutosten ei nähdä palauttavan virastoa enää yhdysvaltalaisten kollaboraatiotyökalujen käyttäjiksi (Lindström, 2022).

Suomalaiset julkiset organisaatiot joutuvat siis todennäköisesti myös tarkastelemaan nykyisille yhdysvaltalaisille pilvipalveluille korvaavia vaihtoehtoja. Tämän pro gradu -tutkielman kirjallisuuskatsaus pyrkii muodostamaan selkeän käsityksen viranomaisvaatimusten asettamista rajoitteista ja vaatimuksista koskien edellä esitellyn kaltaisia tuotteita. Tutkielma rajataan tarkastelemaan kollaboraatiotyökaluja, joita myös edellä esitellyt Microsoft Office / 365, Googlen tuotteet sekä Slack edustavat. Edelleen, tutkielma rajataan käsittelemään vain suomalaisia julkisia organisaatioita, jotka kuitenkin ovat vain eräs vaihtoehtoisista kollaboraatiotyökaluista kiinnostunut joukko. Motivaationa aiheen valinnalle ja rajaukselle toimii myös tutkielman tekijän työnantajan ja tämän asiakkaiden (suomalaiset julkiset organisaatiot) tarpeet ymmärtää tutkittavaa ongelmaa. Työtä ei kuitenkaan ole tehty toimeksiantona tekijän työnantajalle, eikä tutkielman tekijä ole työskennellyt julkisen sektorin kollaboraatiotyökaluja koskevissa projekteissa.

Aihe on kiinnostava myös tieteellisesti. Kollaboraatiotyökaluja koskevaa tutkimusta, saati niiden viranomaissäädännön mukaisuutta koskevaa tutkimusta on julkaistu hyvin vähäinen määrä. Parhaassa tapauksessa tämä tutkielma tulee täyttämään tutkimusaukkoa sekä tuottamaan käytännön hyötyä Suomen julkiselle sektorille ja sen teknologiatoimittajille.

1.3 Tutkimusongelma

Suomalaisilla julkisilla organisaatioilla on tarve käyttää tietoturvallisia kollaboraatiotyökaluja, jotka eivät altista työkaluissa käsiteltyjä henkilötietoja (tai muutakaan dataa) niihin eri tavoin kohdistuville riskeille. Turvallisuuden varmistamiseksi työkalujen täytyy olla vähintään Suomessa pätevän lainsäädännön (kuten yleisen tietosuoja-asetuksen) ja viranomaisvaatimusten (kuten tulkinnat yleisestä tietosuoja-asetuksesta) mukaisia. Lisäksi julkisten organisaatioiden toimintaan vaikuttaa viranomaisohjeistus, kuten Kyberturvallisuuskeskuksen tai valtiovarainministeriön pilvipalveluiden käyttöä koskevat ohjeistukset. Tämän tutkielman aihe on ”Julkisten organisaatioiden kollaboraatiotyökalut ja viranomaisvaatimusten täyttyminen Suomessa”, ja tutkielma pyrkii vastaamaan seuraaviin tutkimuskysymyksiin:

1. Mitä vaatimuksia ja haasteita kollaboraatiotyökalujen hyödyntämiseen liittyy suomalaisissa julkisissa organisaatioissa?
2. Mitä vaatimuksia lainsäädäntö ja viranomaisohjeistus asettavat julkisen organisaation käyttämälle kollaboraatiotyökalulle?
3. Miten organisaatiot voivat varmistaa viranomaisvaatimusten mukaisuuden kollaboraatiotyökaluja valitessaan?

Tämän tutkielman teoriaosuudessa, kirjallisuuskatsauksessa, oletetaan löydettävän vastauksia ennen kaikkea ensimmäiseen kysymykseen. Toiseen kysymykseen saadaan vastauksia sekä kirjallisuuskatsauksesta että tutkimusosuudesta. Kolmanteen kysymykseen tullaan vastaamaan tämän tutkielman lopputuotoksella, eli design-tutkimuksen tuottamalla artefaktilla.

1.4 Käsitteet

Tässä luvussa tarkastellaan tutkielmassa käytettäviä käsitteitä. Osa käsitteistä ei ole vakiintuneita, joten ne saattavat olla määritelty vain tätä tutkielmaa varten, eivätkä siten vastata täysin muualla esiintyvää käyttöä. Joihinkin käsitteisiin pureudutaan vielä tarkemmin niitä koskevassa teoriasisällössä.

Julkinen organisaatio on julkiseen sektoriin kuuluva organisaatio. Suomen Tilastokeskus määrittelee julkisen sektorin seuraavalla tavalla:

> Julkiseen sektoriin kuuluvat valtio ja kunnat. Valtiosektoriin luetaan valtion hallinto, yliopistot, Kansaneläkelaitos, valtion liikelaitokset ja sosiaaliturvarahastot. Kuntiin ja kuntayhtymiin luetaan kunnan hallinto, kunnallinen koululaitos, kuntien ja kuntayhtymien palvelulaitokset ja toimipaikat, jotka eivät ole yhtiömuotoisia, kuten terveyskeskukset, sairaalat, päiväkodit sekä kuntien ja kuntayhtymien liikelaitokset.
>
> (Tilastokeskus, 2020)

Tämän tutkielman kannalta kiinnostavia julkisen sektorin organisaatioita ovat esimerkiksi Kansaneläkelaitos, valtion virastot, sosiaali- ja terveysalan toimijat sekä kunnat kouluineen ja laitoksineen. Tällaisiin toimijoihin viitataan tutkielmassa julkisina organisaatioina.

Pilvipalvelu on käsitteenä laaja-alainen, mutta se ymmärretään hyvin yleisesti palveluna, jonka käyttö tapahtuu internetin välityksellä siten, että kaikki palveluun liittyvä tiedon prosessointi ja varastointi tapahtuu palveluntarjoajan palvelimilla. Standardisoinnin puutteesta huolimatta pilvipalvelut kyetään jaottelemaan jo hyvin totutusti kolmeen palvelumalliin IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service) (Ghazouani & Slimani, 2017). Tässä tutkielmassa keskitytään SaaS-mallilla toimitettuihin pilvipalveluihin eli verkon ylitse käytettäviin sovelluksiin. SaaS-mallin palveluissa käyttäjän

vastuulla ei ole ylläpidettävää infrastruktuuria tai ohjelmistoja, vaan palvelun-tarjoaja vastaa kaikesta muusta kuin itse palvelun käytöstä.

Henkilötiedoksi määritellään yleisessä tietosuoja-asetuksessa kaikki tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyvät tiedot. Näitä tietoja ovat esimerkiksi nimi, henkilötunnus, kotiosoite, puhelinnumero, sähköpostiosoite, IP-osoite, puhelimen sijaintitiedot tai selaimen evästetiedot. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016)

Kollaboraatiotyökalu on heikosti määritelty käsite, ja sitä vastaavia termejä saattavat olla myös yhteistyösovellus, tiimityösovellus tai ryhmätyösovellus. Ruotsiksi käytetään mm. termiä samarbertverktyg ja englanniksi saatetaan puhua collaborative softwaresta tai harvemmin groupwaresta. Tässä tutkielmassa kollaboraatiotyökalulla tarkoitetaan palvelua, joka mahdollistaa käyttäjien keskinäisen pikaviestinnän, ääni- ja videopuhelut, tiedostojen jakamisen sekä yhteiset työtilat. Kollaboraatiotyökalujen ominaisuuksiin kuuluu myös videokonferenssiominaisuudet, joihin saattaa itse videokonferenssin lisäksi lukeutua mm. aulatoiminto, valkotaulutoiminto tai mahdollisuus tehdä kyselyitä ja äänestyksiä.

Yleinen tietosuoja-asetus eli **General Data Protection Regulation (GDPR)** eli EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS (EU) 2016/679 on kaikkia Euroopan unionin jäsenmaita sellaisenaan sitova lainsäädäntö. Yleinen tietosuoja-asetus kumoaa aiemman vuonna 1995 säädetyn tietosuojadirektiivin ja on oleellinen osa Euroopan unionin henkilötietojen suojelua, liikkuvuutta ja henkilöiden oikeuksia. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016)

Schrems II eli **Euroopan unionin tuomioistuimen tuomio asiassa C-311/18** koskee tietosuoja-aktivisti Maximillian Schremsin Facebookia vastaan nostamasta valituksesta tehtyä ennakkoratkaisupyyntöä. EU:n tuomioistuin antoi tuomionsa heinäkuussa 2020 ja kumosi sillä Euroopan unionin kansalaisten henkilötietojen siirrot Yhdysvaltoihin sallineen Privacy Shield -järjestelyn. Käytännössä Schrems II -päätöksellä tarkoitetaan siis Privacy Shieldin kumoamista ja siten Euroopan unionin kansalaisten henkilötietojen siirtämisen kieltämistä Yhdysvaltoihin ilman mallisopimuslausekkeita (ja sittemmin vakiolausekkeita). (Euroopan unionin tuomioistuin, 2020)

Mallisopimuslausekkeet ja **vakiolausekkeet** eli **Standard Contractual Clauses** eli **SCC,** ovat Schrems II -tuomion jälkeen ainoa tapa siirtää Euroopan unionin kansalaisten henkilötietoja Yhdysvaltoihin. Suomessa käsitteellä **mallisopimuslauseke** viitataan yleensä vanhoihin, vuoden 1995 tietosuojadirektiivin aikana säädettyihin lausekkeisiin, joiden siirtymäaika päättyi vuoden 2022 loppuun. **Vakiolausekkeella** puolestaan tarkoitetaan pääsääntöisesti uusia, kesäkuussa 2021 päivitettyjä lausekkeita, jotka on uudistettu vastaamaan Schrems II vaatimuksia.

Englanniksi niin vanhoista kuin uusistakin lausekkeista käytetään termiä Standard Contractual Clauses (SCCs).

Vakiolausekkeet ja aiemmin mallisopimuslausekkeet ovat lausekkeita, joita organisaatiot voivat sisällyttää henkilötietojen siirtoa koskeviin sopimuksiinsa. Vakiolausekkeet määräävät tiedonsiirron molempien osapuolien velvoitteet ja niiden käyttämisen edellytyksenä on tapauskohtainen arviointi tietosuojan tasosta EU:n ulkopuolisessa kohteessa. Näin käytettynä lausekkeiden on tarkoitus taata EU:n edellyttämän tietosuojan taso sopimuksia koskevissa siirroissa. Vakiolausekkeita ei saa muuttaa, mutta niiden vaatimuksien lisäksi voidaan tapauskohtaisen arvioinnin myötä vaatia täydentäviä suojatoimia. (Euroopan komissio, 2021)

Lainsäädäntöjohdannainen riski tarkoittaa tämän tutkielman kontekstissa ennen kaikkea henkilötietojen suojaan kohdistuvaa riskiä, jonka aiheuttaa toisen valtion lainsäädäntö. Liikenne- ja viestintävirasto Traficomin julkaisema Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri) määrittelee lainsäädäntöjohdannaisen riskin tiivistetysti seuraavalla tavalla:

> Lainsäädäntöjohdannaisilla riskeillä viitataan eri maiden lainsäädännössä oleviin mahdollisuuksiin velvoittaa pilvipalveluntarjoaja toimimaan yhteistyössä kyseisen maan viranomaisten kanssa, ja tarjoamaan esimerkiksi suora tai epäsuora pääsy pilvipalvelun asiakkaiden salassa pidettäviin tietoihin. Lainsäädäntöjohdannaiset riskit voivat ulottua sekä salassa pidettävän tiedon fyysiseen sijaintiin että muun muassa toisesta maasta käsin hallintayhteyksien kautta toteutettavaan tietojen luovutukseen. Lainsäädäntöjohdannainen tietojen luovuttaminen ja tutkimusoikeus on useissa maissa rajattu koskevaksi poliisia sekä tiedusteluviranomaisia
>
> (Liikenne- ja viestintävirasto Traficom, 2019)

1.5 Tutkielman rakenne

Tämän tutkielman keskeisin sisältö jakaantuu tätä johdantoa seuraavissa luvuissa käsiteltäviin kirjallisuuskatsauksesta muodostuvaan teoriaosuuteen, tutkimusmenetelmän esittelyyn sekä varsinaisesta tutkimuksesta koostuvaan empiiriseen osuuteen.

Tutkielman toinen luku, kollaboraatiotyökalut ja lainsäädäntö, tulee käsittelemään ensiksi kollaboraatiotyökaluja. Koska kollaboraatiotyökalut tyypillisesti ja perustellusti tuotetaan pilvipalveluina, tässä alaluvussa tutustutaan myös pilvipalveluihin yleisellä tasolla, sisältäen etenkin SaaS-palvelumallilla toimitetut palvelut. Kollaboraatiotyökalujen jälkeen tutustutaan niitä koskevaan lainsäädäntöön ja viranomaisohjeistukseen niin Euroopan unionin kuin suomalaisenkin lainsäädännön osalta. Näiden kahden osa-alueen perusteella pyritään tunnistamaan ja luomaan synteesi julkisten organisaatioiden kollaboraatiotyökaluihin vaikuttavaan lainsäädännöstä ja viranomaisohjeistuksesta.

Teoriaosuuden jälkeen siirrytään tutkielman empiiriseen osuuteen, jota koskeva tutkimusmenetelmä esitellään sille omistetussa luvussaan. Tutkimusmenetelmän jälkeen esitellään itse tutkimuksen toteutus kaikkine vaiheineen ja lopputuloksineen. Varsinainen tutkimustulos, artefakti, on esitelty liitteessä 1.

Viimeinen luku, yhteenveto, kokoaa tutkielman keskeiset havainnot ja tulokset vielä kerran yhteen. Lisäksi tässä luvussa käydään läpi tutkimukseen liittyvät mahdolliset rajoitteet, jatkotutkimusaiheet ja pohdinnat.

2 KOLLABORAATIOTYÖKALUT JA LAINSÄÄDÄNTÖ

Tässä luvussa tarkastellaan tutkielman aihealueen teoriapohjaa sekä lainsäädäntöä ja viranomaisohjeistusta. Luvun tarkoitus on luoda kattava käsitys kollaboraatiotyökaluista ja kollaboraatiotyökaluihin vaikuttavasta lainsäädännöstä sekä viranomaisvaatimuksista. Lopuksi muodostetaan synteesi siten, että ymmärretään mitä lainsäädäntö ja viranomaisohjeistus edellyttää julkisten organisaatioiden kollaboraatiotyökaluilta ja kääntäen, mikä takaa kollaboraatiotyökalun soveltuvuuden suomalaisen julkisen organisaation käyttöön.

Kirjallisuuskatsausta edeltäneen lähteiden kartoittamisen aikana kävi ilmi, että puhtaasti kollaboraatiotyökaluihin keskittyvää tutkimusta on hyvin rajallinen määrä. Koska kollaboraatiotyökalut tavanomaisesti tuotetaan pilvipalveluina, riittävän tieteellisen lähdeaineiston koostamiseksi kollaboraatiotyökaluihin sovellettavaa aineistoa päädyttiin keräämään laajemmin pilvipalveluihin ja SaaS-palveluihin liittyvästä kirjallisuudesta. Tutkielman aineistona käytetään myös lakitekstejä ja muuta viranomaisohjeistusta sekä aihealueeseen liittyviä lakeja koskevia tieteellisiä julkaisuja.

Tieteellisen aineiston kerääminen aloitettiin hakusanoilla ”collaboration tool”, ”cloud service”, ”cloud computing”, ”saas”, ”gdpr”, ”schrems II”, ”compliance”, sisältäen myös hakusanojen mahdolliset monikkomuodot. Hakuja tehtiin seuraavista kirjastoista ja tietokannoista:

- AIS Electronic Library (AISeL)
- Scopus
- ProQuest
- IEEE Xplore
- ACM Digital Library
- Google Scholar

Hakutuloksista valittiin harkintaa käyttäen aiheeseen soveltuvat julkaisut, joista koostettiin ensimmäinen erä syvemmin tarkasteltavaa aineistoa. Tämän aineiston lähteistä löydettiin edelleen merkittävä määrä kirjallisuuskatsaukseen

sopivaa ainestoa sekä vihjeitä joihinkin täsmähakuihin. Kirjallisuuskatsausta edeltänyt aineiston keruu tuotti arviolta 80 – 90 julkaisua, joista lopulta hyödynnettiin alle puolta. Ainestoa karsittaessa suosittiin Julkaisufoorumin mukaan laadukkaina tunnettuja julkaisuja.

2.1 Kollaboraatiotyökalut, SaaS, pilvipalvelut

2.1.1 Pilvipalvelut

Organisaatioissa, kuten yksityisessäkin käytössä, yleisimmin käytetyt kollaboraatiotyökalut toimitetaan tavanomaisesti pilvipalveluna. Tarkemmin näiden pilvipalveluiden palvelumallina (joskus myös toimitusmalli tai jakelumalli) toimii säännönmukaisesti SaaS-malli (Software as a Service). Suomessa julkisen sektorin pilvipalveluiden käyttöä ohjeistava valtiovarainministeriö on tunnistanut tämän yleisemmällä tasolla, ja pilvipalveluiden käyttöä koskevassa ohjeistuksessaan todennut seuraavaa:

> Vahva trendi on, että yleiskäyttöiset, toimialariippumattomat valmisjärjestelmät siirtyvät lähes yksinomaan SaaS-palveluiksi. Paikallisesti (on-premise) asennettavia valmisjärjestelmiä on todennäköisesti hyvin heikosti enää saatavissa 3-5 vuoden päästä.
>
> (Valtiovarainministeriö, 2020)

Kollaboraatiotyökalut ovat malliesimerkki näistä yleiskäyttöisistä, toimialariippumattomista valmisjärjestelmistä. Tämän trendin vuoksi tässä tutkielmassa luodaan katsaus myös pilvipalveluihin ja SaaS-malliin, jotka määrittävät oleellisesti kollaboraatiotyökaluja.

”Pilveä” voidaan kuvailla ja määritellä monella tavalla, ja siitä saatetaan puhua pilvilaskentana, pilvipalveluna tai vain pilvenä. Vaikka pilven ajatus on toteutunut jo 1960-luvun isokoneympäristöissä (mainframe), nykyisen pilven synnyn voi ajoittaa 2000-luvun alkuun (Kavis, 2014). Tuolloin nykyisinkin merkittävimmät pilvipalveluiden tarjoajat Amazon ja Google alkoivat kehittää ja vuonna 2006 julkaista ensimmäisiä pilvipalveluitaan (Google Docs ja Amazon Elastic Computing Cloud, EC2). Käsite pilvilaskenta (cloud computing) lienee esitelty samana vuonna Googlen silloisen toimitusjohtaja Eric Schmidtin toimesta (Qian ym., 2009), kyseistä termiä voidaan pitää synonyyminä pilvelle.

Yhdysvaltalainen merkittävä alan standardoija NIST (National Institute of Standards and Technology) on esittänyt pilvilaskennan määritelmän, jota niin tieteellinen kirjallisuus kuin kaupalliset toimijatkin, sekä myös suomalaiset viranomaistahot usein siteeraavat. Tässä määritelmässä pilvilaskentaan sisältyy tietyin pilvilaskennalle määrätyin ominaisuuksin niin palvelimet ja verkot, kuin tallennuskapasiteetti, sovellukset ja palvelutkin (Mell & Grance, 2011). Määritelmän mukaan pilvilaskenta on malli, jolla on viisi ominaispiirrettä: itsepalvelumalli, verkon yli saatavuus, pilviresurssien jakaminen yhteisestä

resurssivarannosta, elastisuus sekä palvelun mitattavuus (Mell & Grance, 2011). Joissakin yhteyksissä pilvitallennus (cloud storage) kuitenkin saatetaan eriyttää käsitetasolla pilvilaskennasta, mutta tässä tutkielmassa pilvitallennusta ei erotella pilvilaskennasta tai pilvestä.

Suomalaisittain suositumpi termi pilvipalvelu (cloud service) on englanninkielisessä maailmassa heikommin määritelty käsite, joka kuitenkin monesti esiintyy pilvilaskennan synonyymina. Edellä mainitussa NIST:n määritelmässä mainitaan pilvi-infrastruktuuri (cloud infrastucture) kokoelmana laitteistoja ja ohjelmistoja, jotka mahdollistavat määritelmän mukaisen pilvilaskennan, ja edelleen kyseiset laitteistot resursseina, jotka ovat välttämättömiä pilvipalveluiden tarjoamiseksi (Mell & Grance, 2011). Pilvilaskentaa itsessään on saatettu kuvata myös palveluna, esimerkiksi arkkitehtuurina, joka toimittaa laskentaresursseja palveluna (Freet ym., 2015). Toisaalta sillä voidaan viitataan niin palveluina internetin yli toimitettuihin ohjelmistoihin, kuin myös niitä palveluna tarjoaviin laitteisiin ja ohjelmistoihin (Armbrust ym., 2010). Tämän tutkielman kannalta tärkeää on ottaa huomioon, että suomen kielessä termi cloud computing käännetään pilvipalveluksi, eikä termiä pilvilaskenta juuri käytetä, eikä suositetakaan tässä tarkoituksessa käytettäväksi (Euroopan interaktiivinen termipankki, 2016; Sanastokeskus ry, 2016). Vahvistavana esimerkkinä suomalaisen viranomaistahon käyttämästä termistöstä, Traficomin alainen Kyberturvallisuuskeskus on käyttänyt edellä esitettyä NIST:n cloud computingin määritelmää esitellessään pilvipalveluiden ominaispiirteitä (Liikenne- ja viestintävirasto Traficom, 2019).

Tähän työhön liittyvän tutkimuksen aihealueessa, lainsäädännössä ja viranomaisohjeistuksessa sekä suomalaisessa termistössä käytetään yleisesti termiä pilvipalvelu, joten sitä suositaan myös tässä tutkielmassa. Jatkossa pilvipalvelulla siis viitataan kaikkeen, mitä kirjallisuudessa pilvilaskennalla (cloud computing), pilvipalvelulla (cloud services) tai pilvellä (cloud) tarkoitetaan.

2.1.2 Pilvipalveluiden palvelu- ja toteutusmallit

Pilvipalveluita voidaan jaotella niiden palvelumallin (service model) ja toteutusmallin (deployment model) mukaan. Palvelumallit jaetaan tyypillisesti SaaS-, PaaS- ja IaaS-palvelumalliin (Eid ym., 2015; Kavis, 2014; Mell & Grance, 2011; Qian ym., 2009; Wulf ym., 2021), mutta näiden perinteisten mallien lisäksi on esitelty mm. BPaaS (Business Process as a Service) (Grati ym., 2017; Woitsch & Utz, 2015) ja kaiken kattava XaaS (Everything as a Service), jonka alle voi sijoittua edellä mainittujen lisäksi lähes rajaton joukko palvelumalleja, kuten FaaS, CaaS tai BaaS (Duan ym., 2015). Tämän tutkimuksen aihealueessa ei kuitenkaan ole tarpeen esitellä kuin perinteiset palvelumallit, joista edelleen keskitytään pääasiassa SaaS-malliin.

Pilvipalveluista kattavin ja yleensä myös kallein palvelumalli IaaS (Infrastructure as a Service) tarkoittaa virtualisoidun laskentakapasiteetin, tallennustilan, verkkojen tai muun tietoteknisen resurssin tarjoamista verkon ylitse. Pilvipalvelun käyttäjällä on tässä palvelumallissa eniten kontrollia ja joustavuutta palveluna tarjottaviin resursseihin, kuten virtuaalikoneisiin, joita käyttäjä pystyy

hallinnoimaan käyttöjärjestelmätasolla asti. Pilvipalvelun tarjoajan vastuulle jää vain itse konesali fyysisine laitteineen sekä palveluna tarjottavien resurssien virtualisointi. (Eid ym., 2015; Kavis, 2014; Mell & Grance, 2011; Wulf ym., 2021)

Keskimmäinen mutta toisaalta vähiten kulutettu palvelumalli on PaaS (Platform as a Service). Tässä mallissa pilvipalvelun tarjoaja vastaa IaaS vastuiden lisäksi virtualisoidusta laskentakapasiteetista, tallennustilasta, verkkoasetuksista tai käyttöjärjestelmätasosta. PaaS-palvelun käyttäjä kuitenkin pystyy yleensä vaikuttamaan rajallisesti pilvipalvelun tarjoajan hallinnoimien tasojen asetuksiin. Tätä palvelumallia hyödynnetään yleisesti ohjelmistojen kehitystyön ja tarjoamisen alustana, pilvipalvelun kuluttajan keskeisin vastuu onkin itse ohjelmistossa, jota PaaS-resurssilla, alustalla, ylläpidetään (hostataan). (Eid ym., 2015; Kavis, 2014; Mell & Grance, 2011; Wulf ym., 2021)

SaaS, eli Software as a Service, on pilvipalvelun kuluttajan näkökulmasta rajoitetuin ja vähiten muokattavissa oleva palvelumalli. Kirjaimellisesti tämä palvelumalli tarkoittaa ohjelmiston tarjoamista palveluna, jolloin pilvipalvelun kuluttajan ei tarvitse asentaa ohjelmistoa omille laitteilleen. Ohjelmisto sijaitsee siis pilvipalvelun tarjoajan konesaleihin sijoitetuilla palvelimilla. Pilvipalvelun käyttäjän vastuulle jää vain sovelluskohtaisen datan ja asetusten hallinta, sovellusta käyttävien päätelaitteiden hallinta sekä käyttäjänhallinta. (Eid ym., 2015; Kavis, 2014; Mell & Grance, 2011; Wulf ym., 2021)

Ohjelmistotalot ovat jo viime vuosikymmenellä alkaneet suosia SaaS-mallilla toimitettuja ohjelmistoja perinteisten paikallisesti suoritettavien, lisensoitujen ohjelmistojen ylitse, ohjelmistojen toimittaminen pilvestä on tuolloin jo tunnistettu olevan voittava malli (Cusumano, 2010). SaaS-mallissa niin ohjelmiston käyttäjä, että toimittaja hyötyvät tasaisemman ja ennustettavamman hinnoittelun lisäksi laskentatehon mielekkäämmästä allokoimisesta, käyttäjä säästyy ohjelmiston ylläpitämiseltä, testaamiselta, päivittämiseltä ja kustomoinnilta sekä mahdollisesti sen toimittamiseen vaadittavan laitteiston hankkimiselta ja ylläpitämiseltä (Aleem ym., 2021; Cusumano, 2010).

Vastapainona SaaS-mallin selkeisiin hyötyihin, käyttäjät saattavat tunnistaa palvelumallissa myös varjopuolia. Pilvestä verkon yli toimitettu ohjelmisto on luonnollisesti altis verkon häiriöille, ohjelmiston käyttö voi siis estyä käyttäjästään riippumattomista syistä (Cusumano, 2010). Pilven ja käyttäjän välissä olevan verkon lisäksi ohjelmistoa toimittava konesali saattaa epäonnistua tarjoamaan ohjelmiston vaatimaa suorituskykyä esimerkiksi yllättävissä kysyntäpiikeissä. Ohjelmiston toimittaminen omista konesaleista ei ole altis tällaisille riskeille, joille varsinkaan liiketoimintakriittisiä ohjelmistoja ei haluta altistaa.

Ongelmia voidaan kohdata myös ohjelmistojen käyttöönottoon liittyen. Kun ohjelmiston käyttö muuttuu paikallisesti toimitetusta ohjelmistosta SaaS-malliin, sen toimittaminen ei enää vaadi (eikä yleensä mahdollista) kustomointia. Joissakin tapauksissa organisaatiot kuitenkin saattavat kokea tarpeelliseksi kustomoida ohjelmistojaan ja varsinkin niiden datan säilytysratkaisuja, mutta SaaS-malli ei välttämättä mahdollista tätä (Cusumano, 2010). Toimituksen jäykkyys voi siis hankaloittaa SaaS-malliseen toimitukseen siirtymistä, edellyttämällä

mahdollisesti muiden järjestelmien ja prosessien muokkaamista, tai pahimmillaan estää sen.

Kustomoimattomuuden lisäksi SaaS-mallilla toimitetun ohjelmiston käyttäjä ei pysty vaikuttamaan sovelluksen käyttämän datan tallennusmenetelmiin, salaukseen tai sijaintiin (Aleem ym., 2021; Cusumano, 2010). Datan turvallisuudesta huolehtiminen on oleellinen SaaS-mallin hyödyntämiseen liittyvä haaste, jonka toteuttamisesta yritykset ovat myös vaatineet toimittajilta yksityiskohtaisiakin vastauksia. Ohjelmistojen käyttäjien voi olla hyvin vaikea saada tietoa esimerkiksi ohjelmistoihin liittyvistä tietoturvahäiriöistä (security incident) tai moniasiakasympäristöissä (multi-tenant) sijaitsevan datan eristämisestä (Aleem ym., 2021).

Palvelumallien väliset erot liittyvät erityisesti palveluntarjoajan ja palvelun käyttäjän vastuisiin sekä hinnoitteluun. Laajemmat vapaudet palveluna tarjottaviin resursseihin ja joustavuus tuovat käyttäjälle enemmän vastattavaa sekä palvelulle hintaa. Rajatummat vapaudet ja vähäinen joustavuus sallivat palveluntarjoajan optimoida toimitusta, jolloin palvelun käyttäjälle jää vähemmän vastuita ja maksettavaa palvelusta. Kuviossa 1 on esitetty esimerkki mahdollisesta pilvipalveluiden vastuunjakotaulukosta, joka havainnollistaa palvelumallien eroja palveluntarjoajan ja käyttäjän vastuiden näkökulmasta. On kuitenkin syytä huomata, että vastuiden jakaminen riippuu niin palveluntarjoajasta kuin palvelustakin, eikä pilvipalveluille siis ole olemassa yksiselitteistä vastuunjakomallia.

	IaaS	PaaS	SaaS
Data ja informaatio			
Käyttäjät ja pääsynhallinta			
Sovelluksen asetukset			
Sovellus			
Verkkoasetukset			
Käyttöjärjestelmä			
Virtualisointi			
Fyysinen verkko ja laitteet			
Konesali			

Selite	
Asiakas	
Palveluntarjoaja	

KUVIO 1 Pilvipalveluiden vastuunjakotaulukko

Palvelumallien lisäksi pilven luokitteluun sisältyy myös jako toteutusmalleihin (deployment models). Tyypillisesti ja mm. NIST:n standardin mukaan toteutusmalleja on neljä: julkipilvi (public cloud), yksityinen pilvi (private cloud), yhteistöllinen pilvi (community cloud) ja hybridipilvi (hybrid cloud) (Eid ym., 2015; Freet ym., 2015; Mell & Grance, 2011; Qian ym., 2009). Joissakin tapauksissa

toteutusmalliksi on laskettu myös monipilvi (multi-cloud), jolla tarkoitetaan usean pilvipalvelun tarjoajan palveluiden yhtäaikaista käyttöä.

Yleisin ja tunnetuin pilven toteutusmalli on julkipilvi, jolla tarkoitetaan kenen tahansa ostettavissa ja käytettävissä olevaa pilveä. Suurimmat kaupalliset pilvipalvelut, kuten Amazon Web Services, Google Cloud ja Microsoft Azure edustavat tunnetuinta joukkoa tästä toteutusmallista, mutta julkipilvi voi olla myös valtiollisen tai akateemisen toimijan tarjoamaa. (Eid ym., 2015; Mell & Grance, 2011)

Yksityinen pilvi puolestaan tarkoittaa organisaation itse omasta datakeskuksestaan omille käyttäjilleen toteuttamaa pilveä. Pilvipalvelun voi toteuttaa organisaatio itse, tai kolmas osapuoli, mutta pilvipalveluita ei voi käyttää muut kuin organisaation omat ”asiakkaat”. Yksityinen pilvi voi myös sijaita joko organisaation omissa tiloissa, tai muualla. (Armbrust ym., 2010; Eid ym., 2015; Mell & Grance, 2011)

Yhteisöllinen pilvi on ikään kuin laajennettu yksityinen pilvi, jonka käyttäjät koostuvat tietystä joukosta pilvipalvelun käyttäjiä, mutta eivät rajoitu yhteen organisaatioon. Tämä joukko voisi jakaa yhteisiä intressejä liittyen esimerkiksi lakiteknisiin tai tietoturvaan liittyviin vaatimuksiin. Yhteisöllisen pilvipalvelun tarjoaja voi olla kolmas osapuoli tai yksi tai useampi yhteisöllisen pilven käyttäjistä. (Mell & Grance, 2011)

Hybridipilvi on kahden tai useamman edellä mainitun pilven yhdistelmä, joiden välillä on mahdollistettu datan liikkuminen (Mell & Grance, 2011). Hybridipilven oleellisia hyötyjä on mahdollistaa julkipilven hyödyntäminen organisaation kuitenkin säilyttäessä paikallista prosessointia ja säilyttämistä vaativat sovellukset ja data omilla palvelimillaan.

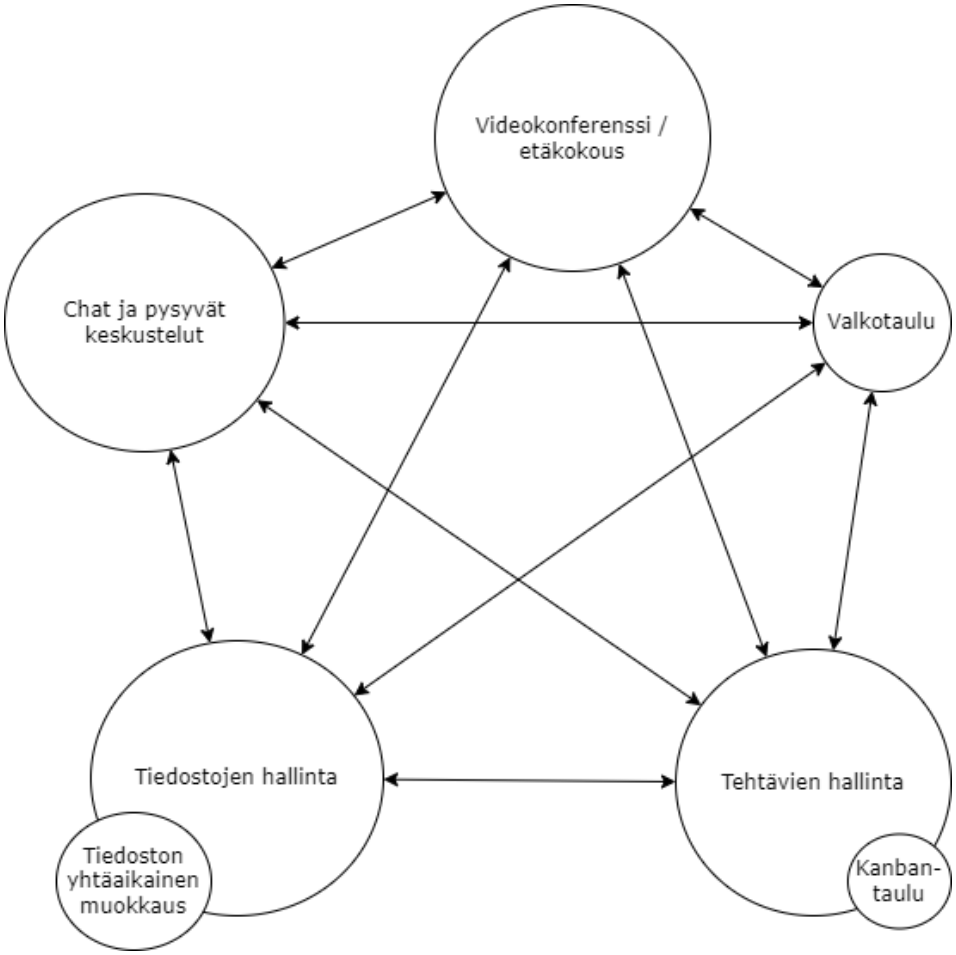
2.1.3 Kollaboraatiotyökalut

Kollaboraatiotyökalut eivät ole kirjallisuudessa yleinen, saati määritelty käsite. Termistön tasolla kirjallisuudessa korostui termin ”groupware” suosio 90-luvulla, kun taas 2000-luvun puolella on siirrytty suosimaan termiä ”collaborative software”. Kollaboraatiotyökaluja tai -ohjelmistoja koskeva kirjallisuus kuitenkin keskittyy lähinnä työkaluihin ohjelmistoina tai itse kollaboratiivisen työn välineenä.

Tässä tutkielmassa mukaillaan sitä koskevan tutkimuksen motiivien johdosta erään julkisen toimijan, ruotsalaisen eSam-verkoston, määritelmää ”digitaalisesta kollaboraatioalustasta”, joka tässä tapauksessa voi koostua yhdestä tai useammasta kollaboraatiotyökalusta (Anderson ym., 2021). Tämä määritelmällinen kollaboraatioalusta sisältää seuraavat toiminnallisuudet, joiden keskinäiset yhteydet on myös visualisoitu kuviossa 2:

- Videokonferenssi (joskus myös etäkokous)
- Tiedostojen tallennus
- Pysyvät keskusteluhuoneet/chat-tilat
- Kanban-taulu

- Valkotaulu



KUVIO 2 Kollaboraatioalusta eSam-verkoston mukaan (Anderson ym., 2021)

eSamin selvitystyössä on esitelty myös esimerkkejä tiedosta, joita julkisen organisaation kollaboraatiotyökaluissa mahdollisesti käsitellään ja varastoidaan. Tällaista suojattavaa, eli selkeää tiedonhallintaa edellyttävää dataa voi olla mm. käyttäjärekisterien sisältämät tiedot, etätapaamisten materiaalit, tilastodata, tietokannat, analyysit, sopimukset sekä myös järjestelmien ja tapahtumien lokitiedot. Lisäksi selvityksessä on tunnistettu etenkin kansalaisten käyttämän kollaboraatiotyökalun käyttäjäkokemuksen merkitys sekä kollaboraatioalustan teknisiin ominaisuuksiin liittyviä seikkoja kuten mukautettavuus, skaalattavuus, muihin palveluihin integroitavuus, tunnistautumisratkaisut ja perinteisin puhelinyhteyksin kokouksiin osallistuminen. (Anderson ym., 2021)

Malliesimerkkejä nykyisin julkisten organisaatioiden käyttämistä kollaboraatioalustoista ovat Google Workspace-palvelut ja Microsoftin 365 -tuoteperhe, joista jälkimmäiseen sisältyy erityisesti kollaboraatiotyökalut Teams ja Sharepoint sekä jo yleisestä käytöstä poistunut Skype. Näiden palveluiden oleelliset toiminnallisuudet liittyvät juuri pysyviin keskusteluhuoneisiin, tiedostojen

tallennus- ja jako-ominaisuuksiin sekä videopuhelu ja -konferenssitoimintoon, molemmat tarjoavat myös valkotaulutoiminnon. eSamin määritelmän mukaisessa kollaboraatioalustassa mainitut Kanban-taulut sen sijaan eivät sisälly Microsoftin tai Googlen yleisimpiin kollaboraatiotyökaluihin. Muita esimerkkejä yleisessä käytössä olevista, mutta suppeammista kollaboraatiotyökaluista ovat mm. etäkokoustyökalu Zoom sekä keskustelualusta Slack.

Kuten todettua, kollaboraatiotyökaluille tyypillistä on niiden toimittaminen pilvestä SaaS-palvelumallilla. Kollaboraatiotyökalun tuottamista pilvipalveluna voidaan perustella mm. sujuvammalla tiedostojen hallinnalla ja monipuolisemmilla yhteistyöominaisuuksilla. Tiedostojen hallinnan puolesta puhuu mm. se, että tiedostoista ei tarvitse kuin yhden kopion, jota kaikki siihen oikeutetut pystyvät käsittelemään. Samoin tässä mallissa käyttöoikeuksien hallinta ja mahdollinen tiedostoja koskevien tapahtumien lokitus on helppoa ja ylipäätä mahdollista. ”Perinteisellä” mallilla tiedostosta luotaisiin kopioita, joiden elinkaarta, ajantasaisuutta, lukuoikeuksia tai tapahtumia on huomattavan paljon vaikeampaa hallinnoida. Yhteistyöominaisuuksia, joita pilvipalveluna toteutettu kollaboraatiotyökalu tarjoaa, ovat mm. jaettavat kalenterit ja tavoitettavuustiedot sekä keskustelualusta- ja palaveritoiminnot. (L, 2022)

Yleisimpien yhdysvaltalaisyritysten tarjoamien kollaboraatiotyökalujen tapauksessa näiden pilvipalveluiden toteutusmallina toimii julkinen pilvi, mutta muita pilvipalvelun toteutusmalleja ei vaihtoehtoisten kollaboraatiotyökalujen tapauksessa pidä sulkea pois. Muiden toimitusmallien puolesta puhuu mm. eräs julkipilven mukana kulkeva riski, joka liittyy julkipilven toimittajan omistajanvaihdokseen. Vaikka julkinen organisaatio valitsisikin lainsäädäntöä silmällä pitäen eurooppalaisen julkipilvipalvelun toimittajan, mutta ei voi varmistua, ettei kyseistä toimittajaa myydä esimerkiksi yhdysvaltalaiselle toimijalle, kollaboraatiotyökalun käyttöön voi tällaisen tapahtuman myötä syntyä uusia tietoturvariskejä.

eSam-verkoston selvitystyön juuret ovat Ruotsin veroviraston ja ulosottoviraston tarpeessa korvata poistuva Microsoftin Skype saman palveluntarjoajan Teamsilla. Ongelmaksi muodostui se, että Microsoft ei tarjoa Teamsia kuin SaaS-mallilla omasta julkipilvestään, eivätkä virastot nähneen sitä toimintaansa ohjaavan regulaation sallimana ratkaisuna. Lisäksi virastot tunnistivat Teamsiin liittyvän riskejä toimittajaloukkuun, hinnoitteluun, jatkuvuuteen, soveltuvuuteen ja jatkuviin muutoksiin liittyen. eSam ryhtyi tämän selvitystyön ajamana etsimään yhdestä tai useammasta kollaboraatiotyökalusta muodostettavaa ratkaisua, joka soveltuisi julkisen sektorin käyttöön. Työtä tuki 121 julkisen sektorin organisaation muodostama referenssiryhmä ja sen tuloksia tulee hyödyntämään käytännössä koko Ruotsin julkinen sektori. (Anderson ym., 2021)

Virastojen alkuperäisestä haasteesta johtuen eSamin selvitys sulki pois yhdysvaltalaisten toimijoiden pilvestään toimittamat ratkaisut, ja tunnisti sekä kokonaisia ratkaisuja, että osaratkaisuja kollaboraatioalustan tarpeelle. Kaksi tunnistettua kokonaisvaltaista ratkaisua ovat avoimeen lähdekoodiin perustuva Nextcloud sekä ruotsalaisen kaupallisen toimijan pilvipalveluna toimittama Compliant Office. Molemmat ratkaisut ovat verrannollisia Microsoftin 365-

tuoteperheeseen sekä Googlen Workspaceen. Siinä missä kollaboraatioratkaisu IceWarpiin perustuva Compliant Office on ruotsalaisista konesaleista tuotettava kaupallinen tuote, Nextcloud on avoimeen lähdekoodiin perustuva teknologia, jota hyödyntämällä palveluntarjoajat voivat tuottaa asiakkailleen kollaboraatiotyökaluja mieleisellään tavalla. Tähän ratkaisuun ovat jo päätyneet mm. Euroopan unionin digitaalista suvereniteettia edistävä GAIA-X -ohjelma, Deutche Telekom ja Ranskan valtio. Molemmat työkalut tarjoavat edellä esiteltyjen ominaisuuksien lisäksi mm. sähköpostin, kalenterin ja tehtävälistat. (Anderson ym., 2021)

Kokonaisvaltaisten kollaboraatiotyökalujen lisäksi kollaboraatioalustan voi kasata pienemmistä työkaluista. Eräs esimerkki tällaista ”komposiittiratkaisusta” on ruotsalaisen Redpill Linpron hahmotelma, jossa ratkaisu koostuu viidestä eri palvelusta. eSamin työssä tunnistettuja, yhtä tai useampaa kollaboraatioalustan ominaisuutta tarjoavia tuotteita ovat mm. Element, Rocket.Chat, Mattermost, Jitsi, Pexip, Cisco Meeting ja Storegate. Selvityksessä on tunnistettu näiden tuotteiden haaste vastata organisaatioiden tarpeeseen järjestää suuria, yli tuhannen osallistujan etätapaamisia, mutta muutoin näiden vaihtoehtoisten kollaboraatiotyökalujen nähdään pystyvän täyttämään organisaatioiden vaatimukset. (Anderson ym., 2021)

Kaiken kaikkiaan kollaboraatioalustalle tai kollaboraatiotyökaluille julkisten organisaatioiden käytössä pystytään tunnistamaan useita vaatimuksia ja huomioon otettavia näkökohtia. Kollaboraatiotyökaluihin liittyvien valintojen merkitystä korostaa työkalujen jopa kriittinen rooli julkisten organisaatioiden sisäisessä ja ulkoisessa viestinnässä, varsinkin kun kollaboraatiotyökaluissa käsitellään suojattavaa dataa. eSamin työ tekee myös selväksi sen seikan, että vaihtoehtoiset, niin kaupalliset (suljetut), kuin avoimeen lähdekoodiin perustuvat kollaboraatiotyökalut ovat täysin varteenotettava vaihtoehto totutuille yhdysvaltalaisten palveluntarjoajien tuotteille.

2.2 Lainsäädäntö ja viranomaisohjeistus

Suomalaisten julkisten organisaatioiden kollaboraatiotyökalujen, kuten muidenkin pilvipalveluiden, valintaan vaikuttaa niin Euroopan unionin laajuista, kuin kotimaistakin lainsäädäntöä sekä viranomaisohjeistusta. Vaikka oleellisin lainsäädäntö suurilta, ja viranomaisohjeistus joiltakin osin, koskee myös muita organisaatioita, on syytä huomioida että tässä tutkielmassa tarkastelu tehdään vain suomalaisten julkisten organisaatioiden näkökulmasta.

2.2.1 EU:n lainsäädäntö ja digitaalinen suvereniteetti

Kuten todettua, eurooppalaisten suhtautuminen henkilötietojen suojaan on verrattaen vakavaa, sitä voidaan pitää jopa kulttuurisena perintönä. Suomi

luonnollisesti jakaa osana Euroopan unionia sen arvot ja perusoikeudet sekä noudattaa Euroopan unionin lainsäädäntöä, joka osaltaan henkii tätä eurooppalaista käsitystä tietosuojan merkityksestä.

Euroopan unionin lainsäädäntö voidaan jakaa primaari- ja sekundaarilainsäädäntöön (joskus myös primaarioikeus ja johdettu oikeus). Primaarilainsäädännöllä tarkoitetaan EU:n perussopimuksia, jotka määrittävät kaikkea Euroopan unionin toimintaa ja tavoitteita sekä toimivat EU-lainsäädännön lähtökohtana. Tällaisia perussopimuksia ovat mm. Euroopan unionin perusoikeuskirja ja Maastrichtin sopimus (sopimus Euroopan unionista). Sekundaarilainsäädäntö puolestaan on primaarilainsäädännön pohjalta tehtyä lainsäädäntöä, johon kuuluvat asetukset, direktiivit, päätökset, suositukset ja lausunnot. (Euroopan komissio, 2022b).

Sekundaarilainsäädännöstä asetukset ja direktiivit ovat sitovia. Asetukset ovat sellaisenaan kaikkia Euroopan unionin jäsenmaita sitovia, kun taas direktiivit velvoittavat jäsenmaita ottamaan ne osaksi kansallista lainsäädäntöään. Päätökset ovat sitovia säädöksiä, jotka voivat koskea EU-maata, yritystä tai yksityishenkilöä päätöstä koskevassa asiassa. Suositukset ja lausunnot eivät ole sitovia, eikä niistä seuraa oikeudellisia velvoitteita. (Euroopan komissio, 2022b).

Tämän tutkielman kannalta kiinnostavinta primäärilainsäädäntöä on Euroopan unionin perusoikeuskirja, johon niin sekundaarilainsäädännössä, kuin sekundaarilainsäädäntöä tulkitsevassa Euroopan unionin tuomioistuimessakin viitataan. EU:n perusoikeuskirja on julkaistu ensimmäisen kerran poliittisena julistuksena vuonna 2000 ja toisen kerran Lissabonin sopimuksen yhteydessä 2007, jolloin sille annettiin EU:n perussopimuksen status ja oikeudellinen sitovuus (Euroopan unioni, 2007). Nämä muutokset astuivat tosin voimaan vasta vuoden 2009 lopussa kaikkien EU:n jäsenmaiden ratifioitua sopimuksen.

EU:n perusoikeuskirjan on kuvattu sisältävän ”kolmannen sukupolven perusoikeuksia”, joihin mm. tietosuoja lukeutuu. Tietosuojaan liittyvässä sekundaarilainsäädännössä ja sitä tulkitsevassa oikeudessa on erityisesti viitattu perusoikeuskirjan artikloihin 7, 8, ja 47, joista kaksi ensimmäistä ovat perusoikeuskirjassa esitettyjä vapauksia, ja jälkimmäinen lainkäyttöä koskeva oikeus.

Artikla 7 koskee yksityis- ja perhe-elämän kunnioittamista, johon sisältyy jokaisen ”oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan” (Euroopan parlamentti neuvosto ja komissio, 2000). Artikla 8 puolestaan käsittelee henkilötietojen suojaa ja on jaettu seuraavaan kolmeen kohtaan:

1. Jokaisella on oikeus henkilötietojensa suojaan.
2. Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.
3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

(Euroopan parlamentti neuvosto ja komissio, 2000)

Lainkäyttöön liittyvä artikla 47 koskee oikeutta tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen. Tämän tutkielman kontekstissa artiklan oleellisin sisältö kuuluu: ”Jokaisella, jonka unionin oikeudessa taattuja oikeuksia ja vapauksia on loukattu, on oltava tässä artiklassa määrättyjen edellytysten mukaisesti käytettävissään tehokkaat oikeussuojakeinot tuomioistuimessa” (Euroopan parlamentti neuvosto ja komissio, 2000). Mainitut tehokkaat oikeussuojakeinot liittyvät erityisesti henkilötietojen Yhdysvaltoihin siirtämisen hyväksyttävyyteen (Rotenberg, 2020).

Perusoikeuskirjan painetun sanan lisäksi Euroopan unionin toimintaa ohjaamaan on kehittynyt ajatus digitaalisesta suvereniteetista (digital sovereignty). Digitaalista suvereniteettia on konseptina ajettu niin autoritäärisissä kuin demokraattisissakin maissa, eikä sen määritelmä ole käsitteen laajasta ja monipuolisesta käytöstä, toisaalta myös vähäisestä akateemisesta tarkastelusta, johtuen yksiselitteinen. Käsitteen alle voidaan liittää niin Venäjän ja Kiinan kaltaisten autoritääristen valtioiden pyrkimykset vahvistaa vallitsevan poliittisen järjestelmän valtaa ja olemassaoloa, kuin länsimainenkin ajatus tietoturvallisuudesta ja omien kansalaisten henkilötietojen hallinnan säilyttämisestä. (Pohle & Thiel, 2020; Roberts ym., 2021).

Digitaalinen suvereniteetti ei ole konseptin kannattajista liberaalimmankaan esittäjän, Euroopan unionin, esittämänä ollut kritiikitön ajatus (Pohle & Thiel, 2020). Puhuttelevat vastalauseet saattavat hakea ajatukselle vertailukohtaa historiasta, muun muassa keskiajan merkittävästä investituurariidasta (Floridi, 2020), tai toisen maailmansodan termistä ”Fortress Europe”, jolla viitataan Natsi-Saksan miehittämään Eurooppaan. Investituurariidassa kirkko ja maallinen valta taistelivat perinteisemmästä suvereniteetista, oikeudesta valita ja asettaa virkaan kirkon toimihenkilöitä, kuten piispoja. Riita johti käytännössä silloisen Euroopan hajoamiseen, varoittavalla vertauksella kiinnitetäänkin huomiota kysymyksen merkittävyyteen ja huomautetaan tällaisen kiistan voittajan kykenevän vaikuttamaan kaikkien osapuolien elämään, tässä tapauksessa mm. kansalaisten oikeuksiin (Floridi, 2020).

Kiistanalaisuudesta huolimatta Euroopan unioni on viimeistään nykyisen Euroopan komission puheenjohtajan, Ursula von der Leyenin, johdolla alkanut vahvistaa pyrkimyksiään kohti digitaalista suvereniteettia. Merkittävimpinä ajureina pyrkimykselle on esitetty huoli Euroopan unionin kansalaisten, yritysten ja valtioiden kyvystä kontrolloida omaa dataansa, ja toisaalta myös huoli Euroopan riippuvuudesta mm. kiinalaisesta teknologiasta, jonka nähdään altistavan tietoturvariskeille. Tämä eurooppalainen digitaalinen suvereniteetti, joka on myös uudelleensanoitettu ”Euroopan kykynä toimia itsenäisesti digitaalisessa maailmassa”, liittyy erityisesti EU:n taloudelle strategisiksi nimettyihin teknologoihin, kuten 5G-verkkoihin, tekoälyyn ja pilvipalveluihin. (Tambiama, 2020).

Pilvipalveluihin, sisältäen pilvitallennustilan, ja laajemmin datan hallintaan liittyvät pyrkimykset ovat synnyttäneet eurooppalaisen hankkeen GAIA-X, jolla eurooppalaisia pilvi- ja datanhallintakyvykkyyksiä pyritään kehittämään, irroittaen Euroopan riippuvuudestaan ulkopuolisiin pilvipalveluiden tarjoajiin (Roberts ym., 2021; Tambiama, 2020). Digitaalisen suvereniteetin innoittamana

tämä hanke sekä muut Euroopan unionin toimet mm. henkilötietojen suojelemiseksi kertovat eurooppalaisen pilven voivan olla tulevaisuudessa todellinen vaihtoehto ei-eurooppalaiselle pilvelle.

2.2.2 Yleinen tietosuoja-asetus ja oikeuden tulkinnat

Digitaalisen suvereniteetin ajatuksen voidaan nähdä Euroopan unionin primäärilainsäädännön (EU:n perusoikeuskirjan) kanssa vaikuttaneen oleellisesti EU:n merkittävimpään tietosuojaa vahvistavaan tekoon, yleisen tietosuoja-asetuksen (GDPR) luomiseen (Roberts ym., 2021; Tambiama, 2020). Viimeistään yleisen tietosuoja-asetuksen myötä Eurooppa on noussut yksityisyyden ja tietosuojan edelläkävijäksi, mahdollistaen yksityishenkilöiden vahvat oikeudet omaan dataansa ja sen käsittelyyn (Tambiama, 2020). Yleisen tietosuoja-asetuksen merkittävyyttä on vahvistanut sen edeltäjään, tietosuojadirektiiviin, sekä itse tietosuoja-asetukseen liittyvät Euroopan unionin oikeuden Schrems-tuomiot.

Kuten todettua, yleisen tietosuoja-asetuksen säätämistä on ohjannut mm. yksityisyyden merkitys ihmisten perusoikeutena (Goddard, 2017). Yksityisyys liittyy oleellisesti henkilötietojen suojaan, joskaan käsitteet eivät ole synonyymeja, vaikka ajoin esiintyvätkin mm. eurooppalaisessa lainsäädännössä päällekkäin (Politou ym., 2018). Edelleen, yksityisyyttä ei ole yksiselitteisesti onnistuttu määrittelemään, ja sillä voidaankin tarkoittaa niin oikeutta jäädä yksin, kuin kontrollia omista henkilötiedoistaankin (Politou ym., 2018).

Yleisen tietosuoja-asetuksen kirjoitettu sisältö koskee tulkitsijoidensa onneksi yksityisyyden sijaan henkilötietojen suojaa, täsmällisesti kyseessä on asetus luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta. Valitettavasti myöskään henkilötiedon määritelmä ei asetuksen näkökulmasta ole yksiselitteistä (Finck & Pallas, 2020). Asetuksen mukaan henkilötiedoksi luetaan kaikki tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Tavanomaisten henkilötietojen lisäksi tällaisia tietoja voivat olla IP-osoitteet, selaimen evästeet tai sijaintitiedot, mikä myös erottaa eurooppalaisen tulkinnan suppeammasta yhdysvaltalaisesta henkilötiedon määritelmästä (Goddard, 2017). Tunnistettavissa olevana henkilönä puolestaan pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen tai useamman henkilölle tunnusomaisen tekijän perusteella (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Henkilön tunnistettavuus on hyvin haastavaa arvioida, mikä siis johtaa haasteisiin tiedon henkilötiedoksi määrittelemiseksi.

Tämän tutkielman tarpeisiin yleisestä tietosuoja-asetuksesta tarkastellaan ennen kaikkea kollaboraatiotyökalujen luonteen johdosta pilvipalveluita koskevia seikkoja. Julkisten organisaatioiden käyttämissä kollaboraatiotyökaluissa saatetaan käsitellä niin tietoisesti kerättyjä organisaation työntekijöiden ja kansalaisten henkilötietoja, kuin henkilötiedoiksi laskettavia ja pilvipalvelun käyttöön liittyviä henkilötietojakin, kuten IP-osoitteita ja sijaintitietoja.

Yleisessä tietosuoja-asetuksessa henkilötietoja käsitteleviä tahoja katsotaan olevan rekisterinpitäjät (controllers) ja henkilötietojen käsittelijät (processors).

Rekisterinpitäjällä tarkoitetaan tiivistetysti toimijaa, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot, tämän tutkielman tapauksessa julkinen organisaatio. Henkilötietojen käsittelijä puolestaan on taho, joka käsittelee henkilötietoja rekisterinpitäjän lukuun, esimerkiksi pilvipalvelun tarjoaja. Käsittelyllä taasen tarkoitetaan käytännössä kaikkea automaattista tai manuaalista henkilötietoihin kohdistuvaa toimintaa, kuten henkilötietojen keräämistä, tallentamista, käyttöä ja poistamista. (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016)

Tässä tutkielmassa ei ole syytä tarkastella syvällisesti rekisterinpitäjiin liittyviä säännöksiä, koska tutkimuksen kiinnostuksen kohteena ovat kollaboraatiotyökalut, eli yleisen tietosuoja-asetuksen näkökulmasta henkilötietojen käsittelijät. Rekisterinpitäjään liittyen on kuitenkin tärkeää huomata, että rekisterinpitäjä on käytännössä aina vastuussa henkilötietojen käsittelystä ja sen lainmukaisuudesta. Henkilötietojen käsittelijä saattaa olla vastuussa silloin kun se ei ole noudattanut juuri sille osoitettuja velvoitteita tai on toiminut rekisterinpitäjän antaman ohjeistuksen vastaisesti. Yleisessä tietosuoja-asetuksessa myös erikseen määrätään, että rekisterinpitäjä, tämän tutkielman tapauksessa julkinen organisaatio, ”saa käyttää ainoastaan sellaisia henkilötietojen käsittelijöitä, jotka antavat riittävät takeet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi niin, että käsittely täyttää tämän asetuksen vaatimukset ja sillä varmistetaan rekisteröidyn oikeuksien suojelu” (Euroopan parlamentti ja Euroopan unionin neuvosto, 2016). Rekisterinpitäjän velvollisuuksiin kuuluu paitsi henkilötietojen käsittelijän soveltuvuudesta varmistuminen, myös tämän ohjeistaminen ja ohjeistusten ylläpitäminen tietojenkäsittelyn säädöstenmukaisuuden varmistamiseksi, sekä sellaisen sopimuksen tekeminen, joka sitoo henkilötietojen käsittelijää noudattamaan yleisen tietosuoja-asetuksen määräyksiä tämän suorittaessa henkilötietojen käsittelyä rekisterinpitäjän puolesta.

Henkilötietojen käsittelijän kannalta oleellista on ensiksi todeta, että yleistä tietosuoja-asetusta sovelletaan Euroopan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn riippumatta siitä, onko henkilötietojen käsittelijä sijoittautunut Euroopan unioniin vai ei. Euroopan unionin jäsenmaiden lisäksi henkilötietojen siirto on sallittu ilman erillistä lupaa Euroopan talousalueen maihin (Norja, Liechtenstein ja Islanti), joissa yleistä tietosuoja-asetusta noudatetaan sekä sellaisiin kolmansiin maihin, joiden on todettu varmistavan riittävän tietosuojan tason. Listaa näistä vastaavuuspäätöksen saaneista maista ylläpitää Euroopan komissio, ja tältä listalta kirjoitushetkellä löytyvät Andorra, Argentiina, Färsaaret, Guernsey, Iso-Britannia, Israel, Mansaari, Japani, Jersey, Uusi-Seelanti, Sveitsi ja Uruguay sekä Kanada kaupallisten toimijoiden osalta (Euroopan komissio, 2022a).

Yhdysvaltojen puuttuessa tältä vastaavuuspäätöksen saaneiden valtioiden listalta, henkilötietojen siirto on täytynyt järjestää joko Euroopan unionin ja Yhdysvaltojen välisen erillisen sopimuksen sallimana, tai mallisopimus-/vakiolausekkeilla. Yhdysvaltain ja Euroopan unionin välisiä sopimuksia henkilötietojen siirtämisen sallimiseksi on ollut toistaiseksi Safe Harbor sekä Privacy Shield -järjestelyt, mutta nämä molemmat on todettu pätemättömiksi Euroopan

tuomioistuimen antamissa Schrems-tuomioissa. Kirjoitushetkellä henkilötietojen siirto Yhdysvaltoihin on siis sallittua vain vakiolausekkeiden avulla, tai tietosuoja-asetuksessa mainituin erityistilanteita koskevin poikkeuksin.

Yleinen tietosuoja-asetus määrää myös asetuksen soveltamisen valvomisesta. Jokaisessa Euroopan unionin jäsenvaltiossa on oltava vähintään yksi tätä tehtävää suorittava riippumaton viranomainen, jolla on toimivalta yleisen tietosuoja-asetuksen mukaisesti annettujen tehtävien hoitoon ja valtuuksien käyttöön. Suomessa tämä valvontaviranomainen on tietosuojavaltuutetun toimisto, jossa tietosuojavaltuutettu työskentelee.

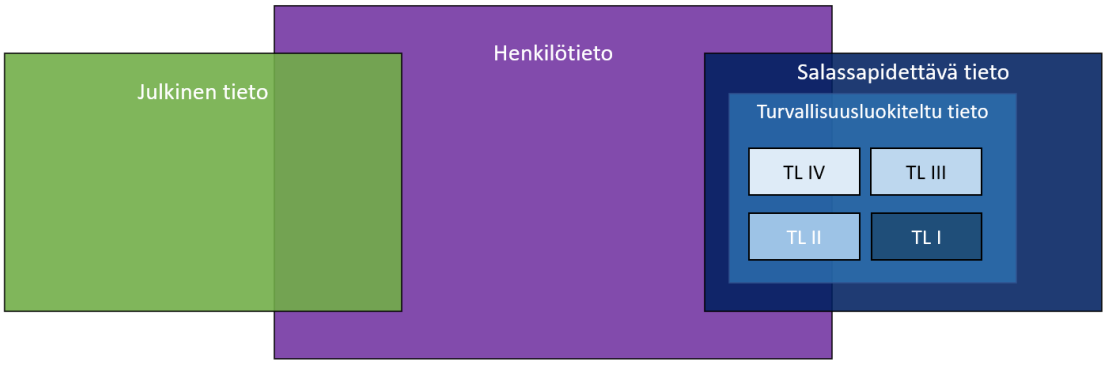
2.2.3 Suomalainen lainsäädäntö ja viranomaisohjeistus

Euroopan unionin laajuisen yleisen tietosuoja-asetuksen lisäksi Suomessa on säädetty kansallista lainsäädäntöä sekä annettu viranomaisohjeistusta, joita julkisten organisaatioiden on otettava mm. kollaboraatiotyökaluja valitessaan huomioon. Kuten todettua, tietosuojavaltuutetun toimisto valvoo ja myös ohjeistaa tietosuojalainsäädäntöön ja henkilötietojen käsittelyyn liittyvissä asioissa, joihin sisältyy myös kansallisesti säädetty tietosuojalaki (1050/2018). Tietosuojalaki täsmentää ja täydentää yleistä tietosuoja-asetusta sekä myös määrää tietosuojavaltuutetun toiminnasta (Eduskunta, 2018). Tämän tutkielman kannalta tietosuojalaki ei kuitenkaan sisällä muuta oleellista lainsäädäntöä.

Laajaan osaan julkista sektoria vaikuttaa myös laki julkisen hallinnon tiedonhallinnasta (906/2019) eli tiedonhallintalaki. Tämän lain tarkoituksiin lukeutuu mm. ”viranomaisten tietoaineistojen yhdenmukainen ja laadukas hallinta sekä tietoturvallinen käsittely” ja ”mahdollistaa viranomaisten tietoaineistojen turvallinen ja tehokas hyödyntäminen”. Käytännössä tiedonhallintalaki velvoittaa viranomaiset järjestämään tiedonhallinnan vaaditulla tavalla, kuten ylläpitämällä tiedonhallintamallia sekä seuraamalla toimintaympäristönsä tietoturvallisuuden tilaa ja varmistamalla tietoaineistojen ja -järjestelmien tietoturvallisuus. (Eduskunta, 2019)

Vaikka tiedonhallintalaki ei suoranaisesti määrää tiedonhallinnan keinoja ja työkaluja, se velvoittaa viranomaisia mm. selvittämään olennaiset tietojenkäsittelyyn kohdistuvat riskit ja mitoittamaan tietoturvallisuustoimenpiteet niiden mukaisesti. Samoin viranomaisen on hankinnoissaan varmistettava, että ”hankittavaan tietojärjestelmään on toteutettu asianmukaiset tietoturvallisuustoimenpiteet” (Eduskunta, 2019). Näiden tietoturvallisuustoimenpiteiden ohjeistuksena saattaa edelleen toimia esimerkiksi valtiovarainministeriön ohjeet julkisen hallinnon pilvipalvelujen hyödyntämiseen, Traficomin kyberturvallisuuskeskuksen julkaisema Pilvipalveluiden turvallisuuden arviointikriteeristö PiTuKri sekä kyberturvallisuuskeskuksen ohjeet pilvipalvelujen turvallisuudesta.

PiTuKri on 11 osa-alueesta koostuva kriteeristö, joka on tarkoitettu suomalaisten viranomaisten työkaluksi pilvipalveluiden turvallisuuden arviointiin. Kriteeristön osa-alueet koostuvat edelleen vaatimuskorteista, joilla osa-alueita jaetaan pienempiin teemoihin. Vaatimuskorttien vaatimukset puolestaan saattavat kohdistua vain osaan suojattavan tiedon tietotyypeistä. Suomalaisten viranomaisten, kuten myös PiTuKrin, käyttämät tietotyypit on esitelty kuviossa 3.



KUVIO 3 Tietotyypit suomalaisessa viranomaiskäytössä (Liikenne- ja viestintävirasto Traficom, 2019)

Pilvipalveluiden kannalta merkittävä tietotyyppien erottelu tapahtuu turvallisuuluokitellun ja ei-turvallisuusluokitellun tiedon välillä. Näistä jälkimmäisen käsittely pilvipalveluissa on vapaampaa, kuin turvallisuusluokitellun tiedon, jonka fyysinen sijainti täytyy olla Suomessa. PiTuKri myös mainitsee, että henkilötietojen fyysisen sijainnin on oltava tietosuojasääntelyn mahdollistamalla alueella. Viranomaisen on tärkeää myös huomata, että suuri määrä salassa pidettävää tietoa tai henkilötietoja voi muodostaa turvallisuusluokitus IV -kasauman, jota tulee käsitellä kuten turvallisuusluokiteltua tietoa. (Liikenne- ja viestintävirasto Traficom, 2019)

PiTuKrin yhdestätoista osa-alueesta ensimmäinen, esiehdot, on tärkein osa-alue. Esiehdot koostuvat kahdesta vaatimuskortista, järjestelmäkuvauksesta (EE-01) ja lainsäädäntöjohdannaisista riskeistä (EE-02). Tämän tutkielman kannalta etenkin jälkimmäinen vaatimus on mielenkiintoinen, sillä se edellyttää pilvipalveluun liittyvien lainsäädäntöjohdannaisten riskien ja velvoitteiden kuvaamista siten, että kuvaus kattaa palvelun käytön ja palvelussa käsiteltävien tietojen koko elinkaaren. Tämän myötä kuvaukselta vaaditaan mm. tieto palvelun käyttöön ja sen tietoihin sovellettavasta lainsäädännöstä ja oikeuspaikasta sekä tieto toimijoista, joilla voi sovellettavasta lainsäädännöstä johtuen olla pääsy palvelussa käsiteltäviin tietoihin. Luonnollisesti nämä kuvatut riskit eivät saa rajoittaa pilvipalvelun sopivuutta tarkasteltavaan käyttötapaukseen. (Liikenne- ja viestintävirasto Traficom, 2019)

Tämän tutkielman kannalta ei ole mielekästä tarkastella syvemmin muita PiTuKrin osa-alueita, joihin lukeutuu mm. vaatimuksia liittyen henkilöstöturvallisuuteen, tietoliikenneturvallisuuteen, fyysiseen turvallisuuteen ja salausmenetelmiin. Jokaisen julkisen organisaation on kuitenkin syytä ottaa pilvipalveluiden turvallisuuden arviointikriteeristö työkaluksi silloin kun organisaation nykyinen tai tuleva kollaboraatiotyökalu toimitetaan pilvestä.

PiTuKrin lisäksi valtiovarainministeriön julkaisut pilvipalveluiden hyödyntämisestä ovat huomion arvoista viranomaisohjeistusta.

Valtiovarainministeriön julkaisu ”Tuottavuutta pilvipalveluilla” esittelee kahdeksan julkisen hallinnon pilvilinjausta, eli pilviperiaatetta, jotka ovat osin yhteneviä PiTuKrin kanssa. Julkaisun mukaan kaikkien julkisen hallinnon toimijoiden tulisi soveltaa näitä pilviperiaatteita omassa toiminnassaan. Pilviperiaatteet on esitelty seuraavassa luettelossa otsikkotasolla. (Valtiovarainministeriö, 2020).

1. Tunnista ja analysoi toiminnallinen tarpeesi, johon etsit ratkaisua
2. Tunnista tietoosi liittyvät keskeiset riskit, tee ratkaisu pilvipalvelun käytöstä faktaperusteisesti
3. Suunnittele ratkaisusi ja siihen liittyvät palvelut alusta asti pilvipalveluja silmällä pitäen
4. Hyödynnä oletusarvoisesti julkisia pilvipalveluja
5. Huolehdi strategisen tiedon ja toimintojen siirrettävyydestä
6. Hyödynnä pilvipalvelun vakio-ominaisuuksia ja automaatiota täysimääräisesti
7. Valvo pilvipalvelun käyttöä
8. Varmista sopimusehtojen soveltuvuus ja varaudu niiden tuomiin riskeihin

Muuta mainitsemisen arvoista viranomaisohjeistusta ovat muut valtiovarainministeriön julkisen hallinnon pilvipalveluiden käyttöä koskevat julkaisut, kuten Julkisen hallinnon pilvipalvelulinjaukset, julkisen hallinnon pilvipalvelujen hyödyntämisen soveltamisohje. Lisäksi PiTuKrin julkaissut kyberturvallisuuskeskus on julkaissut muita pienempiä ohjeistuksiaan pilvipalveluiden käyttöön.

Tässä tutkielmassa ei kiinnitetä huomiota kirjallisuuskatsauksen kirjoitushetkellä lausuntokierroksella olleeseen julkisen hallinnon tietoturvallisuuden arviointikriteeristöön (JulKri). Kriteeristön on tarkoitus toimia organisaatioiden apuna arvioitaessa tiedonhallintalaissa sekä osin tietosuoja-asetuksessa määrättyjä tietoturvallisuutta koskevia määräyksiä. Lähitulevaisuutta ajatellen julkisten organisaatioiden on siis hyvin suositeltavaa ottaa myös tämä kriteeristö huomioon.

2.3 Synteesi

Tässä luvussa esitetyn perusteella voidaan pyrkiä kasaamaan käsitys siitä, mitä julkisten organisaatioiden tulee huomioida kollaboraatiotyökalua valitessaan. Kollaboraatiotyökalulle ei pystytä esittämään selkeää määritelmää, mutta sen keskeisiksi ominaisuuksiksi voidaan tunnistaa ainakin videokonferenssitoiminto, pysyvät keskusteluhuoneet sekä tiedostojen tallennus. Kollaboraatiotyökalulle tyypillistä on sen toimittaminen pilvipalveluna, tarkemmin SaaS-mallilla. Tällaisen pilvipalvelun toteutusmalli sen sijaan voi olla niin julkinen kuin yksityinenkin pilvi, taikka yhteisöllinen pilvi. Toisaalta kollaboraatiotyökaluja voisi toimittaa myös ei-pilvestä, pääasiassa organisaation omilta palvelimilta (on-premises),

mutta tätä vaihtoehtoa ei tarkastella syvemmin sen yhteistyölle rajoitteita synnyttävän luonteen vuoksi.

Jos kollaboraatiotyökalu toteutetaan pilvipalveluna ja siinä käsitellään henkilötietoja, kuten tyypillistä on, julkisen organisaation on otettava huomioon niin Euroopan unionin tasoinen kuin kansallinenkin lainsäädäntö sekä viranomaisohjeistus. Henkilötietojen käsittelyä koskee ennen kaikkea Euroopan unionin yleinen tietosuoja-asetus, joka sitä koskevien Euroopan unionin tuomioistuimen päätöksien myötä asettaa organisaatioille haasteeksi merkittävimpien yhdysvaltalaisten kollaboraatiotyökalujen käytön.

Kotimaisesta lainsäädännöstä julkisten organisaatioiden on huomioitava varsinkin tiedonhallintalaki, joka mm. velvoittaa viranomaisia varmistumaan tietoaineistojen ja -järjestelmien tietoturvallisuudesta. Viranomaisten ollessa lopulta vastuussa tietojenkäsittelyn turvallisuusvaatimusten täyttämisestä, niiden on syytä ottaa huomioon eri tietotyyppejä koskevat ohjeistukset sekä monet pilvipalveluiden käyttöön liittyvät ohjeistukset ja työkalut.

Tämän kirjallisuuskatsauksen havaintojen perusteella voidaan todeta, että julkisen organisaation kollaboraatiotyökalujen valintaa ja käyttöä ohjaa merkittävästi käsiteltävien tietojen tietotyyppi. Jos kollaboraatiotyökalussa käsitellään henkilötietoja, sen hankkiminen esimerkiksi yhdysvaltalaiselta kollaboraatiotyökalujen toimittajilta saattaa muodostaa lainsäädäntöjohdannaisen riskin. Edelleen, jos kollaboraatiotyökalussa käsiteltävät henkilötiedot muodostavat suuren tietokasauman, sitä tulee käsitellä turvallisuusluokiteltuna tietona.

Erityisesti henkilötiedot aiheuttavat organisaatioille haasteita kollaboraatiotyökalujen valinnassa. Sen lisäksi että organisaatio voi havaita datansa muodostavan turvallisuusluokitellun tietokasauman, sillä voi olla haasteita tunnistaa kaikkea käsittelemäänsä henkilötietoa. Jos organisaatio kuitenkin on hankkinut kollaboraatiotyökalun ei-eurooppalaiselta toimittajalta, sen voi olla haastavaa varmistua kaikista yleisen tietosuoja-asetuksen ja mm. pilvipalvelujen turvallisuuden arviointikriteeristön esittämistä vaatimuksista pilvipalvelua kohtaan. Loppu viimein julkinen organisaatio on vastuussa käsittelemästään datasta, jolloin esimerkiksi siihen liittyvien lainsäädäntöjohdannaisten riskien tunnistamistyöstä huolimatta hankittu pilvipalvelu voi osoittautua huomattavaksi riskiksi.

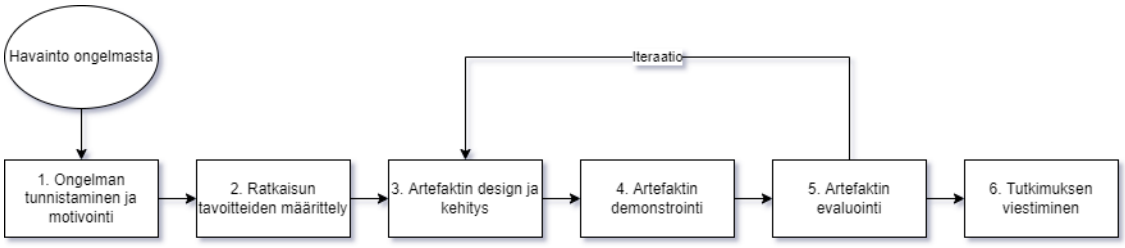
Lakisääteisten vaatimusten ja tietoturvan takaamisen lisäksi kollaboraatiotyökaluihin voi kohdistua vaatimuksia niiden saatavuuden suhteen. Julkisen organisaation on mahdollisesti arvioitava, kuinka merkittäviä häiriöitä kollaboraatiotyökalun saatavuudessa voidaan sallia, ja ottaa nämä vaatimukset huomioon kollaboraatiotyökalua valitessaan. eSam-verkosto nosti esiin myös vaatimuksen palvelun käytettävyydelle, varsinkin jos kansalaiset ovat eräs kollaboraatiotyökalujen käyttäjäryhmä. Tämän lisäksi kollaboraatiotyökaluilta voidaan vaatia monia muita ominaisuuksia, kuten mukautettavuutta, alustariippumattomuutta tai integroitavuutta muihin palveluihin.

3 TUTKIMUSMENETELMÄ

Tutkielman tutkimusosuus toteutettiin design-tutkimuksena, joka tässä luvussa esitellään. Tutkimusmetodi perustuu erityisesti Peffersin ym. (2007) esittelemään prosessimalliin Design Science Research Methology (DSRM), joka koostuu kuudesta vaiheesta. Nämä vaiheet ovat:

1. Ongelman tunnistaminen ja motivointi
2. Ratkaisun tavoitteiden määrittely
3. Artefaktin design ja kehitys
4. Artefaktin demonstrointi
5. Artefaktin evaluointi
6. Tutkimuksen viestiminen

Kuten Peffers ym. (2007) toteavat, DSRM:n mukaista prosessia ei välttämättä suoriteta esitetyssä järjestyksessä, vaan tutkimus saatetaan aloittaa mistä vain vaiheesta välillä 1 – 4. Ensimmäisen vaiheen määrittää tutkimuksen lähtökohdat, mikä luo tarpeen ja motivaation tutkimuksen toteuttamiselle. Tämä tutkimus aloitetaan vaiheesta 1, ongelman tunnistaminen ja motivointi, mikä on tavanomaista, kun tutkimuksen lähtökohtana on havainto tutkittavasta ongelmasta (Peffers ym., 2007). Tutkimusprosessi esitetään kokonaisuudessaan DSRM-malliin sovellettuna kuviossa 4.



KUVIO 4 Tutkimusprosessi

Vaiheet 2 – 6 tulevat seuraamaan vaihetta 1 esitellyssä järjestyksessä. Tunnistetun ongelman määrittely toimii syötteenä ratkaisun tavoitteiden määrittelyllä, joka puolestaan ohjaa tutkimuksessa luotavan artefaktin kehitystä ja designia. Tutkimuksen suunnitteluvaiheessa artefaktin tyylin suhteen ei tehty tarkkaa päätöstä, vaan sen odotettiin alustavasti olevan ongelman ratkaisua ohjaava päätöspuu tai tarkistuslista. Vaihe 4, artefaktin demonstrointi, tarkoittaa tuotoksen teknisen toimivuuden todistamista, toisin sanoen artefaktin kokeilemista yksittäistä kollaboraatiotyökalua vasten, jolloin sen mahdolliset ratkaisupolut ja kirjallinen esitystapa tarkastetaan.

Suunnitelman mukaan artefaktista luotiin alustavasti yksi versio, jota tultiin koestamaan asiantuntijoiden palautteen avulla. Peffers ym. (2007) viittaavat mallissaan Hevnerin ym. (2004) artikkeliin, jonka mukaan design on luonnostaan iteratiivista ja inkrementaalista. Tätä ohjenuoraa noudattaen vaihe 5, artefaktin evaluointi, käsitti paitsi tuotoksen arvioinnin, myös sen mahdolliset iteraatiot ja inkrementoinnin. Evaluointi toteutettiin esittelemällä artefaktia asiantuntijoille, joiden palaute joko validoi artefaktin, tai totesi sen vaillinaiseksi. Jälkimmäisessä tapauksessa prosessin oli määrä iteroitua takaisin vaiheeseen 3, jolloin tuotoksesta luotiin palaute huomioiden seuraava versio. Iteraatiokierroksia tultaisiin tarvittaessa toteuttamaan riittävä määrä, kunnes artefakti todetaan validiksi.

DSRM-prosessin viimeinen vaihe, kommunikointi, vastaa tämän tutkimuksen julkaisemista. Tutkimus toteutettiin pro gradu -tutkielmana, joten sen esittely ja julkaiseminen tapahtui Jyväskylän yliopiston IT-tiedekunnan opinnäytetyötä koskevien ohjeiden mukaisesti (Informaatioteknologian tiedekunta, 2022). Näin ollen tämän tutkielman julkaiseminen Jyväskylän yliopiston julkaisuarkistoon ja siten välittäminen lukijalle toteuttaa tutkimuksen viimeisen vaiheen. Lisäksi tutkielman tekijä saattaa viestiä julkaisustaan myös muissa kanavissa.

4 TUTKIMUKSEN TOTEUTUS

Tämä luku rakentuu kuviossa 4 esitellyn tutkimusprosessin vaiheiden mukaisesti. Jokainen tutkimusprosessissa esitelty vaihe kuvataan vastaavassa alaluvussa, paitsi esivaihe ”havainto ongelmasta”, sitä seuraava ensimmäinen vaihe ”ongelman tunnistaminen ja motivointi sekä viimeinen vaihe ”tutkimuksen viestiminen”. Havainto ongelmasta sekä ongelman tunnistaminen ja motivointi on käsitelty tutkielman johdanto-osuudessa, kun taas tutkimuksen viestiminen toteutetaan tämän tutkielman julkaisuna.

4.1 Ratkaisun tavoitteiden määrittely

Ratkaisun tavoitteiden määrittely mukailee tämän tutkielman viimeistä tutkimuskysymystä ”Miten organisaatiot voivat varmistaa viranomaisvaatimusten mukaisuuden kollaboraatiotyökaluja valitessaan?” Tämän tutkimuksen tavoitteena on siis luoda artefakti, jonka avulla julkisen sektorin organisaatio voi varmistua valitsemansa kollaboraatiotyökalun viranomaisvaatimusten mukaisuudesta.

Artefaktin suunnittelu ja kehitys on määrätietoisempaa, kun sillä on selkeät tavoitteet. Samoin työn onnistumista on helppo arvioida näitä ennalta asetettuja tavoitteita vasten. Ratkaisun tavoitteiden täyttyminen todetaan artefaktin evaluointi -vaiheen jälkeen, kun lopullinen artefakti on hyväksytysti arvioitu aihealuetta tuntevien asiantuntijoiden toimesta ja mahdollisesti muokattu yhden tai useamman iteraation kautta.

4.2 Artefaktin suunnittelu ja kehitys

Artefaktin lopullinen luonne varmistui vasta sen kehitysvaiheessa. Kehitys tapahtui tämän tutkielman kirjallisuuskatsauksen myötä tunnistettujen lakien ja viranomaisvaatimusten yhteen sovittamisella ja niiden koostamisella

eräänlaiseksi tulevan artefaktin esiasteeksi, ottaen huomioon vaatimuksissa kollaboraatiotyökaluihin sovellettavissa olevat kohdat. Tutkimuksen suunnitteluvaiheessa artefaktin todettiin muodostuvan joko päätöspuuksi tai tarkistuslistaksi, joista lopulta päädyttiin jälkimmäiseen.

Tarkistuslistan tunnistettiin olevan monipuolisempi työkalu ei-yksiselitteisten vaatimusten tarkastelemiseen. Artefaktin toteuttaminen päätöspuuna olisi tehnyt artefaktin sisällöstä varsin ehdotonta, mikä tekisi paikoin tulkinnanvaraisiin vaatimuksiin vastaamisesta jopa mahdotonta. Myös lainsäädännön ja viranomaisohjeistuksen eläminen ajan myötä tukee artefaktin toteuttamista tarkistuslistana, jota voi tarvittaessa käyttää vain kussakin ajan hetkessä soveltuvin osin tai versioida kohtuullisella työllä, verrattuna kokonaisuutena tarkasteltavaan päätöspuuhun. Toisaalta päätöspuulla olisi pystytty tarjoamaan selkeämpiä vastauksia silloin kun päätöspuun sisältöön voidaan vastata luontevasti, vastapainona esitystavaksi valittu tarkistuslista jättää organisaation vastuulle enemmän harkintaa ja erilaisten tulkintojen tekemistä. Tämä harkinnanvaraisuus tosin jätetään myös lainsäädännössä ja viranomaisohjeistuksessa organisaation vastuulle, joten samaiseen lakiin ja ohjeistukseen perustuvan päätöspuun on luontevaa tehdä samoin.

Artefaktin kehittämisen aikana kaikesta tunnistetusta viranomaisohjeistuksesta ja laista kerättiin kaikki kollaboraatiotyökaluihin liittyväksi tunnistettu sisältö. Käytännössä tämä tapahtui kopioimalla lakiteksteistä ja viranomaisohjeistuksesta tunnistetut vaatimukset sellaisenaan yhteen tekstitiedostoon. Sisältöä tunnistettiin olevan valtava määrä, joten sitä alettiin kategorisoida jo varhaisessa vaiheessa keskeisiin teemoihin värikoodaamalla tekstitiedostoon kopioituja vaatimuksia. Keskeisen sisällön keräämisen jälkeen todettiin, että tarkistuslistan on syytä käsittää vain keskeisin ohjeistus ja lainsäädäntö, tiivistäen ja koostaen yksittäisiä vaatimuksia laajempien kysymysten alle. Tässä vaiheessa vaatimuksia yhdistettiin teemoittain ja niitä alettiin kirjoittamaan uudelleen tiivistettyjen kysymysten muotoon. Kysymyksiä tiivistettiin laajemmin esitetyiksi kysymyksiksi paikoin useamman kerran. Tämän vaiheen jälkeen kasassa oli ensimmäinen versio varsinaisista kysymyksistä koostuvasta tarkistuslistasta.

Tarkistuslistan kuvaukseen lisättiin myös maininta listasta kevyenä apuvälineenä ja siitä, että lista ei pyri korvaamaan mitään ohjeistusta. Maininta lisättiin, kun havaittiin ettei tarkistuslistalla voida kattavasti käydä läpi kaikkia vaatimuksia ja siten auttaa organisaatioita varmistumaan ehdottomasti kollaboraatiotyökalun vaatimustenmukaisuudesta. Tämä maininta toimii myös samaisesta syystä asetettuna tarkistuslistan vastuunvapautuslausekkeena.

Tarkistuslistan lopulliseksi luonteeksi muodostui esittää organisaatiolle kysymyksiä keskeisimmistä aiheista, kannustaen organisaatiota pohtimaan aihetta ja vastaamaan siihen omasta näkökulmastaan sopivalla tavalla. Listaan sisällytettiin myös maininta rajallisesta mahdollisuudesta käydä läpi turvallisuusluokiteltuun tietoon liittyviä kysymyksiä, ja aiheeseen liittyvät vaatimuksen niputettiin lopulta yhden kysymyksen sisään ”Mikäli kollaboraatiotyökalussa käsitellään turvallisuusluokiteltua tietoa, täyttääkö työkalu turvallisuusluokiteltujen tietojen tiedonhallinta- ja tietoturvallisuusvaatimukset?” Kysymys ohjaa

turvallisuusluokiteltua tietoa käsittelevän organisaation tarkastelemaan turvallisuusluokiteltua tietoa koskevaa suurta joukkoa vaatimuksia.

Tarkistuslistasta, joka on esitelty liitteessä 1, tuli lopulta 19 kohtaa käsittävä lista kysymyksiä, jotka on tutkijan omaa harkintaa käyttäen tiivistetty ja valittu listalla esitettäväksi. Tällaisia kysymyksiä ovat esimerkiksi ”Onko kaikki kollaboraatiotyökalussa käsiteltävän tiedon tietotyypit tunnistettu?” tai ” Onko tiedon ja palveluiden sijaintiin liittyvät riskit tunnistettu ja otettu huomioon?” Tarkistuslistan kysymysten tavoiteltiin olevan keskenään saman syvyistä ja sellaisia kysymyksiä, joita lähdeaineistossa ei sellaisenaan ole esitetty. Tästä huolimatta kysymysten syvyys vaihtelee jonkin verran hyvin ylätasoisista kysymyksistä, kuten edellä esitetyn esimerkin kysymyksessä tietotyypeistä, tarkempiin kysymyksiin, kuten kysymykseen ”Kykeneekö organisaatio keräämään kollaboraatiotyökalusta kaikki vaadittavat lokitiedot?”

4.3 Artefaktin demonstrointi

Artefaktin demonstrointi tarkistuslistan tapauksessa oli varsin yksinkertainen prosessi. Tarkistuslista käytiin läpi kohta kohdalta, pohtien kunkin kohdan arvioitavuutta Microsoft Teams -kollaboraatiotyökalua vasten. Arvioitavalla kollaboraatiotyökalulla ei tässä tapauksessa ollut suurta merkitystä, koska suurin osa kysymyksistä ei liity yksin kollaboraatiotyökaluun, vaan käsittelee mm. kollaboraatiotyökalun toimittajan ja julkisen organisaation välillä tehtävää sopimusta tai julkisen organisaation omia vaatimuksia.

Yksinomaan kollaboraatiotyökaluun liittyvissä kysymyksissä, kuten mahdollisuus lokitietojen keräämiseen tai GDPR-yhteensopivuus, kokeiltiin, tarjoaako kollaboraatiotyökalun palveluntarjoaja kysymyksiin vastaavaa dokumentaatiota tai muita vastauksia. Demonstroinnin aikana selvisi, että Microsoft Teamsin tapauksessa kaikkiin yksin kollaboraatiotyökaluun liittyviin kysymyksiin oli tarjolla vastauksia, joskin vastausten riittävyyden arvioiminen jää julkisen organisaation harkittavaksi.

Tutkimuksessa ei voitu hyödyntää mahdollisia sopimuksia, joita julkisessa organisaatiossa kollaboraatiotyökalun hankintaan liittyen tehtäisiin, mikä osaltaan rajoitti yksittäistä kollaboraatiotyökalua vasten demonstroimista. Lisäksi suurin osa kysymyksistä on arviointia tekevään organisaatioon ja sen itselleen tai ulkopuolelta asetettuihin tarpeisiin liittyviä. Näiden kysymysten osalta demonstrointi toteutettiin pohtimalla, onko kysymys esitetty riittävän selkeällä ja ymmärrettävällä tavalla ja siihen voidaan järkevästi vastata. Jokainen arvioitavissa oleva kohta käytiin läpi edellä mainittujen rajoitteiden puitteissa siten kuin listaa käytännössä hyödyntäessä tehtäisiin, ja niiden todettiin olevan tarkoitukseen sopivia.

Demonstrointivaiheen tärkein sisältö oli artefaktin teknisen toimivuuden todistaminen, mikä toteutui itsearviointina tehdyllä tarkistuslistan sisällön, esitysasun ja esitystavan koestamisella. Demonstroinnin aikana artefaktin keskeistä sisältöä ei muutettu, mutta joitakin tarkistuslistan kysymyksiä asetettiin eri

järjestykseen, jotta tarkistuslistan eteneminen olisi mahdollisimman loogista. Joihinkin kohtiin lisättiin myös jatkokysymyksiä tilanteeseen, jossa organisaation vastaus varsinaiseen kysymykseen on kielteinen. Esimerkiksi palvelun skaalaamiseen ja jatkuvuuteen liittyvän kysymyksen jatkoksi lisättiin jatkokysymys: ”Ellei, onko rajoitteisiin liittyvät riskit hyväksytty?” Tarkistuslistasta korjattiin myös muutamia kirjoitusvirheitä.

4.4 Artefaktin evaluointi

Artefaktin demonstroinnin jälkeen tarkistuslistasta oli luotuna ensimmäinen evaluoitava versio. Artefaktin evaluoimiseksi artefaktia pyrittiin esittelemään sellaisille suomalaisen julkisen sektorin asiantuntijoille, joiden tunnistettiin pystyvän ammatillisella osaamisellaan arvioimaan artefaktin sisältöä. Riittävänä osaamisena pidettiin kokemusta julkisen sektorin organisaatioiden järjestelmistä ja niihin liittyvistä vaatimuksista sekä asiantuntijan itsensä arviota pätevyydestään arvioimaan listan sisältöä. Tämä kokemus saattoi olla kerätty julkisen sektorin toimijan, toimittajan tai soveltuvan kolmannen sektorin toimijan näkökulmasta. Tällaisia asiantuntijoita pyrittiin löytämään hakemalla heitä ensisijaisesti erilaisten julkisen organisaatioiden henkilöstöstä, pääasiassa tietohallinnosta, tai tutkijan henkilökohtaisen verkoston avulla.

Pyyntöjä kommentoida tarkistuslistaa lähetettiin yhteensä 23 ja myönteisiä vastauksia saatiin kolme. Vastaamaan suostuneet asiantuntijat edustivat joko kolmannella sektorilla työskenteleviä julkisen sektorin asiantuntijoita tai yksityisen sektorin toimittajia, joilla oli kokemusta julkisen sektorin teknologiatoimittajana toimimisesta. Artefaktin esittely ja evaluointi tapahtui joko Microsoft Teamsin ylitse tai sähköpostin välityksellä. Asiantuntijoita pyydettiin arvioimaan erityisesti kysymystä ”Onko tarkistuslista validi, eli sitä voi hyödyntää työkaluna kollaboraatiotyökalun viranomaisvaatimusten mukaisuuden arvioinnissa, eikä se sisällä virheitä?” Jos asiantuntija vastasi kysymykseen ”kyllä”, tarkistuslista todettiin validiksi. Lisäksi asiantuntijoita pyydettiin kommentoimaan artefaktia avoimesti, sisältäen tarkistuslistan kehitysehdotukset, mahdolliset puutteet ja muut huomiot.

Artefaktia evaluoitiin yhden kerran jokaisen sitä kommentoimaan suostuneen asiantuntijan kanssa. Kaikilla näistä kerroista artefakti todettiin validiksi, eli sitä voitaisiin hyödyntää suunnitellussa tarkoituksessaan, eikä se sisältänyt virheitä. Lisäksi artefaktiin saatiin useita jatkokehitysehdotuksia koskien listan esitystapaa tai listan hyödyntämistä toisenlaisen työkalun luomiseksi. Listan esitystapaa koskien kehitysehdotuksena esitettiin kysymysten ryhmittely esimerkiksi julkisen organisaation eri vastuualueiden mukaan. Käytännössä tämä voisi tarkoittaa listan räätälöimistä erilaisille julkisille organisaatioille tarkemmin sopivaksi (kunnat, virastot, liikelaitokset, hyvinvointialueet). Listan esitystavaksi ehdotettiin myös sen muuttamista taulukkomuotoon. Taulukkomuotoisesta tarkistuslistasta olisi edelleen mahdollista kehittää RACI-taulukko, joka soveltuisi myös paremmin julkisen organisaation eri osien ja toimijoiden vastuualueiden

kuvaamiseen. Asiantuntijoiden kommenteista kävi ilmi, että erilasten julkisen sektorin organisaatioiden kollaboraatiotyökaluihin liittyvät toiminnot saattavat toimia hyvinkin erilaisin tavoin, jolloin vastuualueiden ryhmittelystä ja taulukoimisesta olisi selkeästi hyötyä.

4.5 Tutkimuksen koonti

Tämän design-tutkimuksen tavoitteena oli luoda artefakti, joka auttaa julkisen sektorin organisaatioita varmistumaan valitsemansa kollaboraatiotyökalun viranomaisvaatimuksen mukaisuudesta. Artefaktin luonne tarkistuslistaksi varmistui vasta siihen liittyvän aineiston tutkimisen jälkeen, keskeinen peruste tälle valinnalle oli viranomaisohjeistuksessa ja lainsäädännössä tunnistettu vastuun siirto organisaatioille. Koska julkinen organisaatio joutuu joissakin tapauksissa itse määrittämään keinot, joilla se täyttää kollaboraatiotyökalua koskevat vaatimukset, on perusteltua että näitä vaatimuksia koostava lista esittää kysymykset samalla tavalla. Osin samasta syystä tarkistuslistasta tuli myös suunniteltua kevyempi apuväline helpottamaan vaatimustenmukaisuuden tarkastelua, sen sijaan että tarkistuslista olisi auttanut julkisia organisaatioita ehdottomasti varmistumaan kollaboraatiotyökalun vaatimustenmukaisuudesta.

Artefaktin kehittämisen jälkeen sitä demonstroitiin koestamalla tarkistuslistaa käytännössä olemassa olevaa kollaboraatiotyökalua vasten. Tätä seurasi artefaktin evaluointi, eli tarkistuslistan antaminen arvioitavaksi asiantuntijoilla. Evaluointivaiheessa artefakti todettiin validiksi ja siihen saatiin myös joitakin jatkokehitysehdotuksia. Valitun tutkimusprosessin mukaista iteraatiovaihetta ei tässä tutkimuksessa toteutettu, koska artefaktin ensimmäinen evaluoitava versio todettiin validiksi. Tutkimusprosessin viimeinen vaihe, tutkimuksen viestiminen, tullaan toteuttamaan tämän tutkielman julkaisemisella.

5 YHTEENVETO

Tämän tutkielman tavoitteena oli perehtyä kollaboraatiotyökaluihin ja niiden käyttämiseen Suomen julkisella sektorilla sekä käyttöön vaikuttavaan lainsäädäntöön ja viranomaisohjeistukseen. Tutkielma pyrki muodostamaan kattavan kuvan näistä aiheista ja luomaan design-tutkimuksen keinoin työkalun helpottamaan julkisia organisaatioita kollaboraatiotyökalua arvioidessaan. Tutkielman tutkimuskysymykset olivat:

1. Mitä vaatimuksia ja haasteita kollaboraatiotyökalujen hyödyntämiseen liittyy suomalaisissa julkisissa organisaatioissa?
2. Mitä vaatimuksia lainsäädäntö ja viranomaisohjeistus asettavat julkisen organisaation käyttämälle kollaboraatiotyökalulle?
3. Miten organisaatiot voivat varmistaa viranomaisvaatimusten mukaisuuden kollaboraatiotyökaluja valitessaan?

Tutkimuskysymyksiin 1 ja 2 vastattiin tutkielman kirjallisuuskatsauksen aikana ja koostetusti luvun 2 synteesissä. Suomalaisten julkisen sektorin organisaatioiden kollaboraatiotyökalujen hyödyntämiseen tunnistettiin liittyvän niin EU:n laajuista kuin kansallistakin lainsäädäntöä sekä kansallista viranomaisohjeistusta. Lisäksi kollaboraatiotyökalujen valintaan saattaa vaikuttaa myös muita motivaattoreita kuten ajatus digitaalisesta suvereniteetista ja vaatimuksia kuten palvelun käytettävyys kansalaiskäyttäjien näkökulmasta tai integraatiot muihin järjestelmiin. Kollaboraatiotyökalujen hyödyntämiseen liittyviksi haasteiksi puolestaan tunnistettiin muun muassa kaikkien käsiteltävien henkilötietojen tunnistaminen, organisaatiolle kuuluvat rekisterinpitäjän vastuut sekä paikoin tulkinnanvarainen lainsäädäntö ja viranomaisohjeistus.

Kirjallisuuskatsauksen tarjottua vastauksia kahteen ensimmäiseen kysymykseen, tutkielma eteni ratkaisemaan kolmatta tutkimuskysymystä. Tähän kysymykseen pyrittiin vastaamaan design-tutkimuksen keinoin luodulla artefaktilla, eli tarkistuslistalla, jota julkisen sektorin organisaatiot voivat hyödyntää tarkastellessaan kollaboraatiotyökalun vaatimustenmukaisuutta. Tarkistuslistan

todettiin olevan toimiva ja hyödyllinen työkalu tehtävässään apuvälineenä, minkä lisäksi tutkimuksen aikana tarkistuslistalle saatiin jatkokehitysideoita.

On kuitenkin huomattava, että tarkistuslista ei toimi kaiken kattavana työkaluna, eikä sillä pystytä täysin korvaamaan mitään olemassa olevaa ohjeistusta. Käytännössä julkisen sektorin organisaatiot voivat siis varmistua kollaboraatiotyökalun viranomaisvaatimusten mukaisuudesta vain tarkastelemalla työkalua kaikkea siihen liittyvää viranomaisohjeistusta vasten. Lisäksi tarkistuslistan hyödyntämisessä on otettava huomioon sen pätevyys vain tietyssä ajan hetkessä. Aihetta koskeva lainsäädäntö ja viranomaisvaatimukset muuttuvat ajan myötä, mikä vuoksi tarkistuslistan sisältö saattaa tulevaisuudessa sisältää vanhentuneita kysymyksiä, tai siitä voi puuttua muuttuneen lainsäädännön tai ohjeistuksen myötä tarpeellisiksi nousseita kysymyksiä. Tarkistuslistaa arvioidessa on myös syytä huomioida tutkimuksen tulosten varmuuteen liittyvä rajoite, joka johtuu varsin vähäisestä määrästä artefaktin evaluointikertoja, eli kommentin antaneita asiantuntijoita.

Tutkimuksen aikana tunnistettiin julkisten organisaatioiden keskenään erilaiset tarpeet ja tavat toimia, minkä myötä eräs mielenkiintoinen jatkotutkimuksen aihe olisi kehittää tarkistuslistaa vielä tarkemmin erilaisten julkisten organisaatioiden käyttöön. Tarkemmin kohdistettu tarkistuslista voisi myös innostaa alan asiantuntijoita osallistumaan lähemmin listan kehitykseen ja validoimaan sitä suuremmissa joukoin. Lisäksi tarkistuslistan käytettävyyden ja hyödyllisyyden arviointi julkisessa organisaatiossa käytännön tilanteessa on hyödyllinen jatkotutkimuksen aihe.

Tämän tutkielman aikana luotiin uutta tietoa kollaboraatiotyökaluista ja niiden hyödyntämisestä suomalaisella julkisella sektorilla. Yleisellä tasolla tutkimusta pilvipalveluiden hyödyntämisestä ja niitä koskevasta Euroopan laajuisesta lainsäädännöstä on tehty varsin runsaasti. Näitä tutkimuksia on myös tässä työssä hyödynnetty tarjoamaan ymmärrystä muun muassa mahdollisista lainsäädännön luomista haasteista ja rajoitteista julkiselle sektorille. Kollaboraatiotyökaluista ei kuitenkaan ole julkaistu merkittävästi varsinkaan tuoretta tutkimusta, joten tutkielman uskotaan tuovan uutta ja päivitettyä tietoa tähän kenttään. Myöskään suomalaisia julkisia organisaatiota ja niiden kollaboraatiotyökaluja koskevia vaatimuksia kokoavaa työtä ei ole aiemmin julkaistu. Tämän tutkielman uskotaan sisältävän niin tieteellisesti kuin käytännössäkin kiinnostavaa uutta tietoa, täyttäen useampaa tutkimusaukkoa.

Tutkielman aikana selvisi, että niin suomalaisilla kuin muillakin eurooppalaisilla julkisilla organisaatioilla on kiinnostusta keinoihin vähentää kollaboraatiotyökaluihinsa kohdistuvia lainsäädäntöjohdannaisia riskejä, joita nykyisiin suosituimpiin kollaboraatiotyökaluihin sisältyy. Lisäksi Euroopan unionin digitaalisen suvereniteetin ajatus kannustaa markkinoita tuottamaan ja organisaatioita suosimaan Euroopassa tuotettuja pilvipalveluita. Ruotsin eSam-verkosto on myös osoittanut, että nykyisille markkinoiden johtaville kollaboraatiotyökaluille löytyy tällaisia vaihtoehtoisia kollaboraatiotyökaluja. Tämän tutkielman toivotaan tarjoavan suomalaiselle julkiselle sektorille työkaluja näiden vaihtoehtoisten kollaboraatiotyökalujen tarkastelemiseen.

LÄHTEET

Aleem, S., Ahmed, F., Batool, R. & Khattak, A. (2021). Empirical Investigation of Key Factors for SaaS Architecture. *IEEE Transactions on Cloud Computing*, *9(3),* 1037–1049. https://doi.org/10.1109/TCC.2019.2906299

Anderson, B., Edwall, K., Einarsson, M., Enocksson, E., Isrealson, S., Nordström, P., Olivestedt, J., Roshanbin, S. & Witt, P. (2021). *Digital collaboration platform for the public sector* (eSam publications). Haettu osoitteesta https://www.esamverka.se/download/18.4a6f5f6917d9204856518c5e/1639137082930/Digital collaboration platform for the public sector.pdf

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, *53(4)*, 50–58. https://doi.org/10.1145/1721654.1721672

Costello, R. Á. (2020). Schrems II: Everything is Illuminated? *European Papers*, *5(2),* 1045–1059. https://doi.org/10.15166/2499-8249/396

Cusumano, M. (2010). Cloud computing and SaaS as new computing platforms. *Communications of the ACM*, *53(4)*, 27–29. https://doi.org/10.1145/1721654.1721667

Datatilsynet. (2022, 14. heinäkuuta). Datatilsynet nedlægger behandlingsforbud i Chromebook-sag. Haettu 7.5.2023 osoitteesta https://www.datatilsynet.dk/afgoerelser/afgoerelser/2022/jul/datatilsynet-nedlaegger-behandlingsforbud-i-chromebook-sag-

Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C. & Hu, B. (2015). Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends. *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, 621–628. https://doi.org/10.1109/CLOUD.2015.88

Eduskunta. (2018). *Tietosuojalaki*. Haettu 7.5.2023 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2018/20181050

Eduskunta. (2019). *Tiedonhallintalaki*. Haettu 7.5.2023 osoitteesta https://www.finlex.fi/fi/laki/alkup/2019/20190906

Eid, M., Al-Jabri, I., Sohail, M. & Syed, K. (2015). Cloud Computing Adoption: A Mapping Of Service Delivery And Deployment Models. *The Fifteenth International Conference on Electronic Business*, 160–165.

Euroopan interaktiivinen termipankki. (2016). *IATE ID: 2250701*. Haettu 7.5.2023 osoitteesta https://iate.europa.eu/entry/result/2250701/all

Euroopan komissio. (2000). *2000/520/EY: Komission päätös*. Haettu 7.5.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32000D0520&qid=1658000855934

Euroopan komissio. (2021). *Standard Contractual Clauses*. Haettu 7.5.2023

osoitteesta https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_fi

Euroopan komissio. (2022a). *Adequacy decisions*. Haettu 7.5.2023 osoitteesta https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_fi

Euroopan komissio. (2022b). *EU-lainsäädännön tyypit*. Haettu 7.5.2023 osoitteesta https://ec.europa.eu/info/law/law-making-process/types-eu-law_fi

Euroopan parlamentti ja Euroopan unionin neuvosto. (1995). *EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI 95/46/EY*. Haettu 7.5.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A31995L0046

Euroopan parlamentti ja Euroopan unionin neuvosto. (2016). *Euroopan Unioni (EU) 2016/679*. Haettu 7.5.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679&from=FI

Euroopan parlamentti neuvosto ja komissio. (2000). *Euroopan unionin perusoikeuskirja*. Haettu 7.5.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:12012P/TXT&from=FI#d1e195-393-1

Euroopan unioni. (2007). *Lissabonin sopimus*. Haettu 7.5.2023 osoitteesta https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=celex%3A12007L%2FTXT

Euroopan unionin tuomioistuin. (2015). *Euroopan unionin tuomioistuimen tuomio (suuri jaosto) 6.10.2015*. Haettu 7.5.2023 osoitteesta https://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=462191

Euroopan unionin tuomioistuin. (2020). *Euroopan Unionin tuomioistuimen tuomio (suuri jaosto) 16.7.2020*. Haettu 7.5.2023 osoitteesta https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FI&mode=lst&dir=&occ=first&part=1&cid=110407

Finck, M. & Pallas, F. (2020). They who must not be identified-distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, *10(1),* 11–36. https://doi.org/10.1093/idpl/ipz026

Floridi, L. (2020). The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy and Technology*, *33(3),* 369–378. https://doi.org/10.1007/s13347-020-00423-6

Freet, D., Agrawal, R., John, S. & Walker, J. J. (2015). Cloud forensics challenges from a service model standpoint: IaaS, PaaS and SaaS. *7th International ACM Conference on Management of Computational and Collective Intelligence in Digital*

EcoSystems, 148–155. https://doi.org/10.1145/2857218.2857253

Ghazouani, S. & Slimani, Y. (2017). A survey on cloud service description. *Journal of Network and Computer Applications*, *91(1 August 2017),* 61–74. https://doi.org/10.1016/j.jnca.2017.04.013

Goddard, M. (2017). Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, *59(6),* 703–706. https://doi.org/10.2501/IJMR-2017-050

Grati, R., Boukadi, K. & Ben-Abdallah, H. (2017). Business adaptation for BPaaS using fuzzy logic systems. *14th International Conference on Computer Systems and Applications*, 645–651. https://doi.org/10.1109/AICCSA.2017.148

Hevner, A. R., March, S. T., Park, J. & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28(1),* 75–105.

Informaatioteknologian tiedekunta. (2022). *Pro gradu -tutkielma*. Haettu 7.5.2023 osoitteesta https://www.jyu.fi/it/fi/ohjeita-opiskelijalle/opiskelu/pro-gradu-tutkielma

Kavis, M. (2014). *Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS)*. New York: Wiley.

L, J. (2022). *The security benefits of modern collaboration in the cloud*. National Cyber Security Centre Blog. Haettu 7.5.2023 osoitteesta https://www.ncsc.gov.uk/blog-post/the-security-benefits-of-modern-collaboration-in-the-cloud

Liikenne- ja viestintävirasto Traficom. (2019). *Pilvipalveluiden turvallisuuden arviointikriteeristö (PiTuKri)*. Haettu osoitteesta https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Pilvipalveluiden_turvallisuuden_arviointikriteeristo_PiTuKri_v1_1.pdf

Lindström, K. (2022, 7. tammikuuta). Nu börjar myndigheterna upphandla Teams-alternativ – och hr-system står näst på tur. *Computer Sweden*. Haettu 7.5.2023 osoitteesta https://computersweden.idg.se/2.2683/1.768071/myndigheter-borjar-upphandla-teams-alternativ--i-host-ska-vi-titta-pa-hr-system

Malmqvist, M. (2022, 20. tammikuuta). Därför säger Stockholms stad nej till Microsoft 365 – ”vill säkerställa att vi följer lagarna”. *Computer Sweden*. Haettu 7.5.2023 osoitteesta https://computersweden.idg.se/2.2683/1.761640/stockholm-nobbar-microsoft-365

Mell, P. & Grance, T. (2011). The NIST Definition of Cloud Computing. *NIST Special Publication 800-145*. Haettu osoitteesta https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Peffers, K., Tuunanen, T., Rothenberger, M. A. & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of*

Management Information Systems, *24(3),* 45–77. https://doi.org/10.2753/MIS0742-1222240302

Pohle, J. & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9(4),* 1–18. https://doi.org/10.14763/2020.4.1532

Politou, E., Alepis, E. & Patsakis, C. (2018). Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions. *Journal of Cybersecurity*, *4(1),* 1–20. https://doi.org/10.1093/cybsec/tyy001

Qian, L., Luo, Z., Du, Y. & Guo, L. (2009). Cloud computing: An overview. *IEEE International Conference on Cloud Computing*, 623–631.

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M. & Floridi, L. (2021). Safeguarding european values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10(3).* https://doi.org/10.14763/2021.3.1575

Rossi, A. (2018). How the Snowden Revelations Saved the EU General Data Protection Regulation. *International Spectator*, *53(4)*, 95–111. https://doi.org/10.1080/03932729.2018.1532705

Rotenberg, M. (2020). Schrems II, from Snowden to China: Toward a new alignment on transatlantic data protection. *European Law Journal*, *26(1–2),* 141–152. https://doi.org/10.1111/eulj.12370

Sanastokeskus ry. (2016). *Tietotekniikan termitalkoot: pilvipalvelu*. Haettu 7.5.2023 osoitteesta https://sanastokeskus.fi/tsk/fi/termitalkoot/hakemistot-267.html?page=get_id&id=ID141&vocabulary_code=TSKTT

Tambiama, M. (2020). *Digital sovereignty for Europe.* European Parliamentary Research Service. Haettu 7.5.2023 osoitteesta https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Tietosuojavaltuutetun toimisto. (2022, 15. helmikuuta). *Tietosuojavaltuutetun toimisto käynnistää selvityksen julkisen sektorin pilvipalvelujen käytöstä osana Euroopan valvontaviranomaisten yhteistä toimenpidettä*. Haettu 7.5.2023 osoitteesta https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-kaynnistaa-selvityksen-julkisen-sektorin-pilvipalvelujen-kaytosta-osana-euroopan-valvontaviranomaisten-yhteista-toimenpidetta

Tilastokeskus. (2020). *Julkinen sektori*. Haettu 7.5.2023 osoitteesta https://www.stat.fi/meta/kas/julkinen_sektor.html

Valtiovarainministeriö. (2020). *Tuottavuutta pilvipalveluilla*. Valtiovarainministeriön julkaisuja 2020:66. Haettu 7.5.2023 osoitteesta https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/162451/VM_2020_66.pdf?sequence=4&isAllowed=y

Woitsch, R. & Utz, W. (2015). Business Process as a Service: Model Based Business and IT Cloud Alignment as a Cloud Offering. *2015 International Conference on Enterprise Systems (ES)*, 121–130. https://doi.org/10.1109/ES.2015.19

Wulf, F., Lindner, T., Westner, M. & Strahringer, S. (2021). IaaS, PaaS, or SaaS? The why of cloud computing delivery model selection - Vignettes on the post-adoption of cloud computing. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 6285–6294. https://doi.org/10.24251/hicss.2021.758

LIITE 1 – TARKISTUSLISTA

Tämän tarkistuslistan kysymykset perustuvat julkisen sektorin kollaboraatiotyökaluihin sovellettavissa oleviin viranomaisohjeistuksiin ja lainsäädäntöön. Tarkistuslistan on tarkoitus toimia kevyenä apuvälineenä kollaboraatiotyökalun viranomaisvaatimusten mukaisuutta tarkastellessa. Lista ei pyri korvaamaan mitään ohjeistusta, vaan se kokoaa keskeisen ohjeistuksen sisällön helposti läpikäytävään muotoon. Varsinkaan salassa pidettäviä tietoja käsitellessä lista ei voi tarjota kattavaa kokoelmaa tarkastettavista kohdista. Kysymysten ei ole välttämätöntä saada selkeitä kyllä/ei -vastauksia, vaan tarkoitus on muistuttaa organisaatiota pohtimaan kysymystä ja sitä, onko vastaus organisaation näkökulmasta riittävä.

Onko kaikki kollaboraatiotyökalussa käsiteltävän tiedon tietotyypit tunnistettu?

Onko mahdollista, että kollaboraatiotyökaluun kasautuu suuri määrä salassa pidettävää tietoa, henkilötietoja tai turvallisuusluokiteltua tietoa?

Mikäli kollaboraatiotyökalussa käsitellään turvallisuusluokiteltua tietoa, täyttääkö työkalu turvallisuusluokiteltujen tietojen tiedonhallinta- ja tietoturvallisuusvaatimukset?

Mikäli kollaboraatiotyökalussa käsitellään turvallisuusluokiteltua tietoa, onko tietoihin kohdistuvat riskit tunnistettu ja arvioitu?

Jos kollaboraatiotyökalussa käsitellään henkilötietoja, säilyvätkö ne GDPR:n määräämällä alueella?

Mikäli henkilötietoja siirtyy GDPR:n määräämän alueen ulkopuolelle, pystytäänkö siirto toteuttamaan mallisopimuslausekkeilla?

Onko tiedon ja palveluiden sijaintiin liittyvät riskit tunnistettu ja otettu huomioon?

Onko lainsäädäntöjohdannaiset ja toimittajan yritysjärjestelyihin liittyvät riskit tunnistettu ja otettu huomioon?

Onko kollaboraatiotyökalulta vaadittavat toiminnalliset tarpeet kaikkien sen käyttäjäryhmien osalta tunnistettu?

Onko näiden tarpeiden mukaiseen toimintaan ja sen tiedonhallintaan liittyvät riskit ja vaatimukset tunnistettu?

Täyttääkö palvelu kollaboraatiotyökalulta edellytettävät saatavuuden ja jatkuvuuden vaatimukset?

Onko mahdollisuus kollaboraatiotyökalun ja sen toimittajan vaihtamiseen / exitiin huomioitu ja siihen varauduttu?

Ellei tietoja ja toimintoja voi tarvittaessa siirtää, onko tarpeen ilmenemiseen liittyvä riskiarvio tehty?

Onko kollaboraatiotyökalun mahdolliset räätälöimisen tarpeet tunnistettu?

Onko kollaboraatiotyökaluun liittyvän valvonnan ja hallinnan vaatimukset tunnistettu ja pystytäänkö ne täyttämään?

Mahdollistavatko sopimusehdot palvelun skaalaamisen molempiin suuntiin, sekä palvelujen jatkuvuuden? Ellei, onko rajoitteisiin liittyvät riskit hyväksytty?

Onko kollaboraatiotyökalun toimittajan oman edut takaavien sopimusten riskit tunnistettu ja niihin varauduttu?

Pystyykö organisaatio varmistamaan, että kollaboraatiotyökaluun on toteutettu kaikki vaadittavat tietoturvallisuustoimenpiteet kollaboraatiotyökalun toimittajan puolelta?

Kykeneekö organisaatio keräämään kollaboraatiotyökalusta kaikki vaadittavat lokitiedot?