Tampereen yliopisto

Jani Kuhno

TIETOTURVA- JA TIETOSUOJAUHAT PILVIPALVELUJA HYÖDYNTÄVISSÄ KIRJASTOJÄRJESTELMISSÄ

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Joulukuu 2019

TIIVISTELMÄ

Jani Kuhno: Tietoturva- ja tietosuojauhat pilvipalveluja hyödyntävissä kirjastojärjestelmissä
Kandidaattitutkielma
Tampereen yliopisto
Tietojenkäsittelytieteiden tutkinto-ohjelma
Joulukuu 2019

Kirjastoilla on resurssipula, jota voidaan lievittää hyödyntämällä pilvipalveluita kirjastojärjestelmässä. Kirjastojärjestelmä mahdollistaa kirjaston perustoiminnan, kuten aineiston lainaamisen ja varaamisen sekä sen löydettävyyden ja hankkimisen. Pilvipalvelut ovat usein uutisissa niihin liittyvistä tietoturva- ja tietosuojaongelmista. On päädytty tutkimaan, mitä tietoturva- ja tietosuojauhkia pilvipalveluja hyödyntäviin kirjastojärjestelmiin liittyy.

Tuloksena on saatu, että on olemassa kolme keskeistä tietoturva- ja tietosuojauhkaa: tiedon omistajuus, yksityisyys ja datakeskuksen sijainti. Näiden yhteisen tekijän on päätelty olevan pilvipalvelun toimittaja. Pilvipalveluiden tietoturvan ja tietosuojan parantamiseksi tulisi kirjaston tehdä palvelutasosopimus, joka tarkasti määrittelee, miten tietoturvaa ja tietosuojaa pyritään turvaamaan ja mitä sanktioita sen rikkomisesta ilmenee.

Tutkimus on suoritettu kirjallisuuskatsauksena, jossa valikoitu aineisto on englanninkielistä ja kansainvälistä, pitkälti Euroopan ulkopuolisista maista. Tuloksia ei voida sellaisenaan yleistää suomalaisiin kirjastoihin.

Avainsanat: tietoturva, tietosuoja, yksityisyys, pilvipalvelut, kirjastojärjestelmä

1 Johdanto

Nykymaailmassa kirjastojen on pysyttävä mukana teknologisessa kehityksessä, jolloin ne pystyvät tarjoamaan parempia ja uusia informaatiopalveluja [Makori, 2016]. Ongelmana on, että kirjastoilla on jatkuva pula resursseista [Abidi ja muut, 2012]. Kustannuksien vähentämiseksi on ehdotettu, että kirjastot ottaisivat käyttöön pilvipalveluja, joko täydentämään nykyistä kirjastojärjestelmää tai kokonaan korvaamaan se [Erturk ja muut, 2015].

Pilvipalveluihin liittyy tietoturva- ja tietosuojahaasteita, jotka estävät niiden varauksettoman käyttöönoton organisaatioissa [Fox, 2009]. Kirjastojen tulisi tiedostaa nämä haasteet ennen palveluiden hankkimista, koska ne käsittelevät sekä suuria määriä hankittuun aineistoon liittyvää dataa että henkilötietoja. Nämä ovat niin asiakkaiden kuin henkilökunnan tietoja, joiden yksityisyys tulisi taata. Tutkielmassa toteutetaan kirjallisuuskatsaus, joka pyrkii kuvaamaan ja arvioimaan pilvipalveluja hyödyntävissä kirjastojärjestelmissä ilmeneviä tietoturva- ja tietosuojauhkia.

Tutkimuksessa käytetyn kirjallisuuden etsimiseen on käytetty Andor, Google Scholar, ProQuest ja Scopus -tietokantoja. Haussa pyrittiin etsimään kirjallisuutta, joka käsittelisi pilvipalveluja hyödyntäviä kirjastojärjestelmiä. Samalla sen tulisi mainita tai käsitellä tietoturvallisuutta. Tämän lisäksi haussa haluttiin rajata, että kirjallisuus olisi tietojenkäsittelytieteiden alainen, koska kyseessä on tietojenkäsittelytieteen tutkielma.

Tietokannoista on etsitty lähdekirjallisuutta hakulausekkeella: (security OR privacy) AND (”cloud-based” OR ”cloud based” OR ”cloud services” OR ”cloud computing”) AND (”library management system” OR ”integrated library system”). Scopuksessa tämä tuotti vain yhden tuloksen, joten hakulauseketta lavennettiin poistamalla (security OR privacy) -lause, mikä tuotti relevantimpia tuloksia. Tämän lisäksi sekä Scopuksessa että Andorissa rajattiin tulokset tietojenkäsittelytieteeseen. Näiden lisäksi on ProQuestista löydetty kirjallisuutta ”Related items” kohdasta ja Google Scholarissa on valittu ”Aiheeseen liittyvät haut” kohdasta ehdotettu hakulauseke ”impact of cloud computing library practices”.

Kirjallisuuden valitsemiskriteereinä ovat olleet pääkäsitteiden, eli ”kirjastojärjestelmät” ja ”pilvipalvelut” sekä ”tietoturva” tai ”tietosuoja” esiintyminen tuloksissa. Aineistoksi on kelpuutettu sellainen kirjallisuus, joka käsittelee yleisesti pilvipalveluja kirjastojärjestelmissä, jos siinä käydään läpi niiden tietoturva- tai tietosuojahaasteita.

Valikoidun kirjallisuuden perusteella on saatu tulokseksi, että pilvipalveluja hyödyntävissä kirjastojärjestelmissä tietoturvauhat ilmenevät tiedon omistajuuden ja yksityisyyden menettämisellä sekä datakeskuksen sijainnin mahdollisista laillisista huolista. Näiden yhteisenä tekijänä on pilvipalvelun toimittaja, joten voidaan päätellä, että tietoturvahaasteisiin vastaaminen tapahtuisi lailla, linjauksilla ja säännöillä. Näitä voi määritellä sekä maan hallitus että pilvipalvelu ja kirjasto palvelutasosopimuksella.

Tutkielmassa ei ole käyty läpi, miten avoin ja suljettu lähdekoodi mahdollisesti vaikuttavat pilvipalvelun tietoturvatasoon. Tämän lisäksi ei tarkastella yhtä tiettyä pilvipalvelua, vaan pyrkimyksenä on ollut luoda yleinen katsaus pilvipalveluja hyödyntävien kirjastojärjestelmien tietoturvauhkiin. Eri kirjastotyyppien vaikutusta tietoturvavaatimuksiin ei tarkastella. On huomioitava, että vaikka kyseessä on suomenkielinen tutkielma, tulokset eivät ole yleistettävissä Suomen kirjastoihin. Lähdekirjallisuus on pitkälti Euroopan ulkopuolisista maista, jolloin niissä ei ole otettu huomioon, esimerkiksi Euroopan Union yleisen tietosuoja-asetuksen vaikutuksia tietoturvaan.

Johdannon jälkeen tutkielma etenee seuraavasti. Luvussa kaksi esitellään pääkäsitteet. Luvussa kolme käydään läpi lähdekirjallisuudesta löydetyt tietoturva- ja tietosuojauhat. Luvussa neljä pohditaan, miten nämä haasteet tulisi ottaa huomioon pilvipalveluja hankittaessa, kuinka yleistettävä tutkielma on, mitä lähdekirjallisuudesta voidaan päätellä, ja mitä jatkotutkimuksia tulisi suorittaa. Lopuksi luvussa viisi tutkielman ongelma ja tulokset nidotaan yhteen.

2 Käsitteet

Tässä luvussa käydään läpi tutkielman pääkäsitteet. Pääkäsitteet ovat kirjastojärjestelmä, pilvipalvelut sekä tietoturva ja tietosuoja.

2.1 Kirjastojärjestelmä

Kirjastojärjestelmien määritelmä vaihtelee eri maiden välillä. Englanninkielessä on olemassa neljä eri lyhennettä, joilla voidaan puhua kirjastojärjestelmistä. Näitä ovat: **ILS** (”integrated library system”), **LMS** (”library management system”), **ILMS** (”integrated library management system”) ja **LSP** (”library services platform”). Suomenkielessä sen sijaan puhutaan joko **kirjastojärjestelmistä** tai **keskitetyistä kirjastojärjestelmistä**.

Kirjastojärjestelmä on tietojärjestelmäkokonaisuus, joka koostuu eri ominaisuuksista, joiden avulla hallitaan kirjaston fyysistä, elektronista ja digitaalista aineistoa. Tämän lisäksi järjestelmän tulee tarjota asiakkaille käyttöliittymä, jolla he

pääsevät selaamaan, hakemaan ja varaamaan kirjastolla saatavilla olevaa aineistoa. Näitä eri kirjastojärjestelmän ominaisuuksia kutsutaan moduuleiksi [Fu ja muut, 2013]. Kirjastojärjestelmän määritelmä sisältää tutkielmassa moduulit **kirjaston hallinnasta, OPAC:ista** ja **verkkokirjastojärjestelmästä** sekä **hakuliittymästä**.

Tämän tutkielman lähdekirjallisuudessa on käsitelty useita eri kirjastojärjestelmiä ja niiden moduuleja. Näitä ovat esimerkiksi ExLibris Alma, ExLibris Primo, BiblioCommons, LibLime Koha, OCLC WorldShare ja Librarika. Nämä kaikki kirjastojärjestelmät ja niiden moduulit ovat pilvipohjaisia. Niitä ei tulla käymään tämän tarkemmin läpi tutkielmassa, koska on haluttu irtautua tarkastelemasta yhtä tiettyä palvelua. Sen sijaan tässä tutkielmassa on pyritty selvittämään yleisesti pilvipohjaisten kirjastojärjestelmien tietoturva- ja tietosuojauhkia. Näin siksi, että yksittäinen pilvipalvelun toimittaja ei tunne, että tässä tutkielmassa löydetyt tietoturva- ja tietosuojaongelmat ovat yksinomaan heidän palvelussa. Sen sijaan tutkielman tavoitteena on antaa sekä kirjastoammattilaisille että pilvipohjaisten kirjastojärjestelmien kehittäjille yleinen näkemys, mitä tietoturva- ja tietosuojahaasteita pilvipalveluita hyödyntäviin kirjastojärjestelmiin liittyy.

Tutkielmassa ei selvitetä, minkälainen vaikutus tietoturvaan ja tietosuojaan on, jos pilvipohjainen kirjastojärjestelmä tai sen yksittäinen moduuli on kehitetty avoimella tai suljetulla lähdekoodilla. Aikaisemmin mainituista kirjastojärjestelmistä LibLime Koha perustuu avoimeen lähdekoodiin, kun taas esimerkiksi ExLibris Alma on kehitetty suljetulla lähdekoodilla.

Kirjaston hallitsemiseen tarvitaan eri **moduuleita** eri tehtäviin. Perustehtävä, jota kirjaston hallinnassa tarvitaan, on kirjaston henkilökunnan ja asiakkaiden välinen viestintä. Viestintä voi tapahtua niin sähköpostitse, tekstiviestin kautta tai verkkokirjastolla olevan chat-palvelun kautta. Viestinnän lisäksi kirjastojen asiakaspalveluun kuuluu asiakkaiden tekemien lainojen ja (seutu)varauksien valvonta sekä kaukolainat ja kotipalvelu. [Axiell Aurora, 2019]

Asiakaspalvelun ohella, kirjastojen hallinnassa tarvitaan ominaisuuksia, joilla käsitellä kirjastoaineiston luettelointia ja indeksointia. [Axiell Aurora, 2019]. Yleisesti kirjastoilla on käytössä MARC (MAchine-Readable Cataloging) 21 -tiedontallennusformaattiin perustuva bibliografinen kuvaus. Aineiston tietueita on mahdollista lukea eri kirjastoissa, eli formaatti mahdollistaa tiedon siirrettävyyden. Kirjastojärjestelmän tulee tukea tätä formaattia. [Ikäheimo, 2019; Axiell Aurora, 2019]

Kirjaston aineistohallintaan tarvitaan sen hankintaprosessia tukevat ominaisuudet. Tähän prosessiin kuuluu aineiston tilaaminen, vastaanottaminen ja laskutus. Näiden ominaisuuksien lisäksi kirjastojärjestelmän tulisi antaa kirjastoammat-

tilaisille mahdollisuus hakea kirjaston aineistoa hakujärjestelmän avulla. Kirjastojärjestelmän tulisi tarjota tilastoja, raportteja ja lokitietoja kirjaston toiminnasta. [Axiell Aurora, 2019]

Kirjaston hallinta koostuu aineiston kierrätyksestä asiakkaan ja kirjaston välillä, kirjaston aineistonhallinnasta, hankintaprosesseista ja asiakaspalvelusta. Näiden lisäksi kirjastojärjestelmän moduuleihin kuuluu kirjaston asiakkaille suunnatut palvelut, jotka auttavat heitä muun muassa hakemaan, varaamaan ja lainaamaan kirjaston aineistoa.

OPAC (online public access catalog) on kirjaston julkinen aineistotietokanta. **Verkkokirjastot** tai **verkkokirjastojärjestelmät** (engl. *digital library*) tarjoavat kirjaston asiakkaille julkisen käyttöliittymän, jolla he pääsevät selailemaan ja tekemään hakuja OPAC:ista. OPAC:in käytön lisäksi verkkokirjastot antavat kirjaston asiakkaiden esimerkiksi lainata, varata, tehdä aineistohankintapyyntöjä ja päivittää käyttäjätietonsa [PIKI-verkkokirjasto ohjeet, 2018]. Verkkokirjastot voivat mahdollisesti toimia samalla mobiilisivustona, joten verkkokirjastojärjestelmän tulisi olla responsiivinen ja mukautua sitä käyttävän laitteen mukaisesti [Axiell Arena, 2019].

Englanninkielessä on kirjastojärjestelmistä eritelty niiden aineiston **hakuliittymä** (engl. *discovery layer*). Tämä ei ole virallinen suomennos, koska kyseinen ominaisuus ei suomalaisissa kirjastoissa ole eritelty omaksi osakseen. Virallista suomennosta ei ole, vaan hakuliittymä on yleisesti luettu osaksi verkkokirjastoa. Hakuliittymä voi koostua eri Web 2.0 ominaisuuksista, jotka pyrkivät lisäämään käyttäjien ja palvelun vuorovaikutusta, yhteistyötä muiden käyttäjien kanssa ja käyttäjien omia tuotoksia [Kritikos ja muut, 2017].

Web 2.0 ominaisuudet ovat jo arkipäivää internetissä. Esimerkiksi Pirkanmaan kirjastojen PIKI-verkkokirjastossa on käyttäjien mahdollista "tägätä" eli luokitella tunnisteilla teoksia sekä lisätä niihin omia arvosteluja [PIKI-verkkokirjasto ohjeet, 2018]. Samalla verkkokirjaston hakujärjestelmä osaa dynaamisesti suositella hakulauseita, kun käyttäjä kirjoittaa hakukenttään. Tällaisten Web 2.0 ominaisuuksien tarkoitus on pyrkiä parantamaan kirjastojen aineiston löydettävyyttä.

2.2 Pilvipalvelut

Pilvipalvelut (engl. *cloud services*) ovat **pilvilaskennalla** (engl. *cloud computing*) toteutettuja internet-palveluita. Pilvilaskennalla tarkoitetaan yhteisiä, internetin kautta toimitettavia tietokoneresursseja, jotka skaalautuvat niiden käyttäjien tarpeiden mukaan. Näitä resursseja hyödynnetään eri pilvipalvelujen kautta. Esimerkiksi Google Drive tarjoaa verkkotallennustilaa käyttäjille, johon he voivat tallentaa esimerkiksi valokuvia tai asiakirjoja [Google Drive, 2019]. Vastaavasti Microsoft Azure tarjoaa yrityksille sovelluskehitys- ja julkaisualustan [Microsoft Azure, 2019].

Pilvipalveluille ominaista on, että palveluun ostetaan käyttöoikeuslisenssi sen toimittajalta [Fox, 2009]. Käyttäjät eivät asenna mitään omille laitteilleen, vaan pilvipalveluja käytetään esimerkiksi verkkoselaimen kautta [Ifijeh, 2014]. Pilvipalveluiden hankinta yrityksille tarkoittaa, että IT-infrastruktuuriin tuodaan mukaan organisaation ulkopuolinen palveluntoimittaja. Tämä siirtäisi osan kirjaston IT-infrastruktuurista sen ulkopuolelle, koska pilvipalveluiden palvelimet sijaitsevat muualla olevassa datakeskuksessa.

Pilvipalvelut jaetaan eri **pilvipalvelutyyppeihin**. Nämä ovat:

- **Software as a Service** (SaaS) -pilvipalvelutyyppi, jossa käyttäjille tarjotaan yksittäinen ohjelma tai ohjelmistokokonaisuus, esimerkiksi Google Drive.
- **Infrastructure as a Service** (IaaS) -pilvipalvelutyypissä pilvipalvelun tuottajalta ostetaan palvelimilta laskentatehoa ja tallennustilaa. Tällöin voidaan ulkoistaa pilvipalveluja hankkivan yrityksen palvelimet ja niiden ylläpito pilvipalvelun tuottajalle. Esimerkiksi Microsoft Azure.
- **Platform as a Service** (PaaS) -pilvipalvelutyyppi on tarkoitettu sovelluskehitykseen, jossa pilvipalvelu tarjoaa mahdollisuudet luoda ja julkaista omia internet-sovelluksia. Esimerkiksi Microsoft Azure.

Pilvipalveluissa tuotettua dataa voidaan säilyttää, joko yrityksen omilla palvelimilla tai hankkia tallennustila pilvipalvelusta. Tällöin tietoja säilövät palvelimet ovat eri palvelinkeskuksessa. Tällaisessa tilanteessa on mahdollista, että datakeskuksessa olevissa palvelimissa on muiden pilvipalvelun asiakkaiden tietoja eli kyseessä on **julkinen pilvityyppi** (engl. *public cloud*) [Ifijeh, 2014]. Sen sijaan, jos yritys haluaa palvelimet vain omaan käyttöönsä, kutsutaan tällaista pilvityyppiä **yksityiseksi pilveksi** (engl. *private cloud*). Jos tällainen ratkaisu toteutettaisiin useiden eri yritysten kesken, kutsuttaisiin sitä **yhteisölliseksi pilveksi** (engl. *community cloud*). Jos muodostetaan pilviratkaisu, jossa on useita eri pilvityyppejä yhdessä, kutsutaan tätä **hybridi pilveksi** (engl. *hybrid cloud*). [Kaushik ja muut, 2013]

Kirjastoille merkittävin hyöty pilvipalveluista on niiden kustannustehokkuus. Kuten alussa on mainittu, kirjastoilla on pula resursseista. Resurssipulaan vaikuttaa kirjastojen jatkuvasti kasvava aineistokokoelma. Nykypäivänä kirjastoilla on tavallisten fyysisten aineistojen viitetietokantojen lisänä digitaalista aineistoa. Pilvipalveluja voidaan hyödyntää tässä, koska niiden tallennustila voidaan skaalata käytön mukaan. Maksetaan vain siitä tilasta, mitä käytetään. [Makori, 2016]

Kirjastojen tallennustilan vaatimuksesta lisääntyvillä palvelinmäärillä on sekä taloudellinen vaikutus että ekologinen. Datakeskukset tuottavat hiilidioksidipäästöjä siinä missä muu elektroniikka. Keskittämällä julkisen pilven alle, yhteiseen palvelinkeskukseen, kirjastot muuntuvat ekologisemmiksi. Palvelimia ei olisi enää

eri kirjastojen ylläpitämissä palvelinkeskuksissa, vaan ne olisivat samassa palvelinkeskuksessa muiden pilvipalvelun asiakkaiden kanssa. Tällöin ne hyödyntäisivät kaikkia asiakkaita, eivätkä olisi käyttämättöminä. [Abidi ja muut, 2012; Goldner, 2010]

Kirjastoammattilaisille pilvipalvelut mahdollistavat helpon jakamisen ja yhteistyön eri kirjastojen välillä. Esimerkiksi Google Docsin käyttämällä he voivat luoda yhdessä asiakirjoja ja jakaa niitä Google Driven kautta. Samalla pilvipalvelut mahdollistavat niiden käytön mistä tahansa ja millä tahansa. Pilvipalveluille ominaista on, että ne ovat itsenäisiä niitä käyttävistä laitteista ja käyttöjärjestelmistä. Ainoa asia, minkä pilvipalveluiden käyttö vaatii, on internet-yhteys. [Tritt ja muut, 2014]

2.3 Tietoturva ja tietosuoja

Suomenkielessä on tehty jako **tietoturvan** (engl. *information security, data security*) ja **tietosuojan** (engl. *information privacy, data privacy, data protection*) välillä. Tämän tutkielman lähdekirjallisuudessa puhutaan usein molemmista käsitteistä samassa tietoturvallisuuden kontekstissa [Stukalova ja muut, 2016; Tritt ja muut, 2014].

Tietoturva ja tietosuoja liittyvät oleellisesti toisiinsa. Tästä esimerkkinä Euroopan unionin tietosuoja-asetus, joka artiklassa 32 on määritellyt, henkilötietojen käsittelyn turvallisuuden takaamisen kontekstissa, että "*kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus*" [EU 2016/679, 2016]. Asetuksen artiklassa määritellään, että tietosuojasta huolehtivan henkilön, organisaation tai ulkopuolisen käsittelijän tulee taata palveluidensa tietoturva. Tietoturva ja tietosuoja ovat molemmat saman henkilön tai organisaation vastuulla ja ovat tämän seurauksena toisistaan erottamattomat organisaatiossa, jossa henkilötietoja ilmenee, kuten kirjastoissa. Tästä syystä tässä tutkielmassa on pyritty selvittämään paitsi tietoturva- että tietosuojauhkia, joita pilvipalveluja hyödyntävissä kirjastojärjestelmissä ilmenee.

Tietoturva eli tietoturvallisuus muodostuu tiedon **eheyden** (engl. *integrity*), **luottamuksellisuuden** (engl. *confidentiality*) ja **saatavuuden** (engl. *availability*) varmistamisesta. Tiedon luottamuksellisuus varmistaa, että tietoa pääsevät käyttämään ja tarkastelemaan vain siihen luvan saaneet tahot. Esimerkiksi pääsynhallinnalla voidaan varmistaa, että tietoihin eivät pääse luvattomat osapuolet. [Traficom, 2019]

Tiedon eheydellä tarkoitetaan tiedon muuttumattomuutta [Traficom, 2019]. Tietoa ei saa muuttaa ilman, että muokkauksesta jää merkintä, eivätkä sitä saa

muuttaa henkilöt, joilla ei ole siihen asianomaista lupaa. Se ei saa muuttua tahattomasti, esimerkiksi ohjelmistollisen tai inhimillisen virheen seurauksena tai tahallisesti tietoturvahyökkäyksen seurauksena.

Tiedon saatavuuden, jota voidaan kutsua käytettävyydeksi, varmistaminen takaa, että tieto on käytettävissä niille asianomaisille, joille on sen käyttöön annettu lupa [Traficom, 2019]. Tieto ei saa kadota ilman, että esimerkiksi sen käyttöluvan omaava henkilö on määrännyt sen tuhottavaksi.

Tietosuojalla tarkoitetaan sellaisten tietojen turvaamista, joilla on mahdollista tunnistaa henkilö. Näitä tietoja on voitu tallentaa esimerkiksi sähköisesti tietokantaan tai fyysisesti paperille. Tällaisia tietoja ovat esimerkiksi, nimi, osoite, sekä puhelinnumero. Näitä tietoja kutsutaan yleisesti henkilötiedoiksi. [Tietosuojavaltuutettu: tietosuoja, 2019; Tietosuojavaltuutettu: henkilötieto, 2019]

Tietosuojaan kuuluvat yksityisyyden lailliset säädökset ja linjaukset. Suomessa näitä määritellään sekä henkilötietolain että EU:n yleisen tietosuoja-asetuksen avulla. Näihin kuuluu oikeus henkilölle, jonka henkilötiedot on tallennettu, saada tietää, miten heidän henkilötietojansa käsitellään ja mahdollisuuksien mukaan pyytää ne poistettavaksi tai korjattavaksi, jos niissä on ilmennyt virheitä. Henkilön tulee saada tietoja henkilötietojen käsittelystä, sitä pyydettäessä. [Opiskelijan digitaidot, 2019]

Kirjastoilla on paitsi henkilötietojen, kuten asiakkaiden- ja henkilökunnantietojen, suojaamisen ja turvaamisen lisäksi laaja määrä muuta tietoa, josta niiden tulee pitää huolta. Yleisissä kirjastoissa näitä ovat esimerkiksi bibliografiset luettelot, lisensoidut aineistot ja mahdollinen digitaalinen aineisto [Wang ja muut, 2011]. Akateemisissa kirjastoissa taas on digitaalisia kopioita, esimerkiksi opinnäytetöistä ja tutkimusraporteista [Yuvaraj, 2015]. Tässä tutkielmassa ei eritellä kirjastoja toisistaan, koska tietoturvauhat ja -riskit kohdistuvat pilvipalveluja hyödyntäviin kirjastojärjestelmiin riippumatta niitä hankkivan kirjaston kirjastotyypistä.

3 Tietoturva- ja tietosuojahaasteet

Tässä luvussa käydään läpi löydetystä kirjallisuudesta ilmenneitä tietoturva- ja tietosuojauhkia, joita kirjastojärjestelmissä pilvipalveluja hyödyntävät kirjastot tulevat mahdollisesti kohtaamaan. Lähdekirjallisuudesta löydettyjen tulosten perusteella, ne on jaettu kolmeen eri tietoturva- ja tietosuojauhkaan: tiedon omistajuus, datakeskuksen sijainti ja yksityisyys.

3.1 Tiedon omistajuus

Tiedon omistajuudella viitataan siihen, että pilvipalveluun tallennettu tieto on kirjaston käytettävissä millä tavoin ja minä aikana tahansa. Tallennettu tieto on saatavilla ja käytettävissä vain niille henkilöille, joilla on siihen käyttöoikeus. Kirjastoissa tämä olisi esimerkiksi kirjastoammattilaisten pääsy aineistotietokantaan. Tiedon tulee pysyä muuttumattomana eli se ei saa muuttua pilvipalvelussa tahattomasti, vaan esimerkiksi käyttöluvan saaneen kirjastoammattilaisen. Pilvipalveluun tallennettua tietoa tulee luvan saaneiden henkilöiden vapaasti tuhota ja siirtää pois palvelusta.

Goldner [2010] toteaa artikkelissaan kirjastoista ja pilvipalveluista, että tiedon omistajuus on yksi huoli, joka kirjastoammattilaisilla on pilvipalveluiden käyttöönotossa. Artikkelissaan hän vaatii, että kirjastoilla tulee olla täydellinen omistajuus omasta tiedosta pilvipalveluissa. Hänen mukaansa kirjastojen tulee päästä käyttämään ja käyttää tietoja tarpeittensa mukaan. Tällaisia tarpeita ovat esimerkiksi pilvipalveluun tallennetun tiedon käyttö muissa palveluissa. Tämän lisäksi kirjaston tulee saada ladattua tietonsa pilvipalvelusta, jos kirjasto esimerkiksi haluaa vaihtaa pilvipalvelusta toiseen. Sama toiminto tulee sekä sallia että mahdollistaa siinä tapauksessa, että pilvipalvelun toimittaja lopettaa toimintansa.

Goldnerin [2010] artikkelista voidaan päätellä, että tiedon omistajuuden menettäminen on tietoturvallinen uhkatekijä. Se vaarantaisi pilvipalveluun tallennetun tiedon saatavuuden ja eheyden. Tietoa, jota kirjasto ei enää hallitsisi itse täysin, voi mahdollisesti päästä käyttämään luvattomat henkilöt. Sen eheyttä ei voida taata, koska tiedosta voi mahdollisesti jäädä kopioita, esimerkiksi tilanteessa, jossa se on määrätty tuhottavaksi. Samanlainen tilanne voi tapahtua silloin, kun tietoa pyritään siirtämään pilvipalvelun ulkopuolelle.

Tiedon siirrettävyys nousee esille Stukalovan ja muiden [2016] suorittamassa kirjallisuuskatsauksessa. Tutkielmassaan he ovat pyrkineet selvittämään pilvipalveluiden hyödyntämistä kirjastoissa. Tätä he ovat tarkastelleet venäläisen ja muiden maiden kirjallisuuden perusteella. Tuloksena he ovat saaneet, että pilvipalveluja valitessa tulee saada tietää, mitä tallennetulle tiedolle tapahtuu, jos pilvipalvelun toimittaja lopettaa toimintansa tai toinen yritys ostaa pilvipalvelun. Tästä voidaan tehdä johtopäätös, että tiedon eheys ja saatavuus ovat vaarassa pilvipalveluun tallennettuna. Tiedon siirtämisessä ei voida olla varmoja, mitä tiedolle tapahtuu. Esimerkiksi jääkö siitä kopioita edellisen pilvipalvelun toimittajalle, jos kirjasto päättää siirtyä toiseen pilvipalveluun.

Tiedon omistajuuteen liittyvät tietoturvallisuushuolet ilmenivät Trittin ja muiden [2014] kirjastoammattilaisille suorittamassa kyselyssä. Kyselyssään he pyrki-

vät selvittämään kirjastoammattilaisten asenteita ja käyttökokemuksia pilvipalveluista sekä minkälaisia vaikutuksia niiden käytöllä on ollut heidän työhön. Kysely suoritettiin Yhdysvalloissa sijaitsevissa pienissä akateemisissa kirjastoissa. Siihen saatiin 120 vastausta, joista 98 nähtiin oikeellisina.

Trittin ja muiden [2014] suorittamassa kyselyssä kirjastoammattilaiset kertovat, että pilvipalveluun tallennetun tiedon saatavuus ja eheys ovat asiat, jotka huolestuttavat heitä pilvipalvelujen käytössä. Tästä voidaan päätellä, että tietoturvallisuus on asia, joka on tärkeää kirjastoammattilaisille. Siihen kohdistuvat uhat, kuten tiedon omistajuuden menetys pilvipalveluja käytettäessä, aiheuttavat levottomuutta kirjastoammattilaisissa.

Saatavuus ja eheys nousivat esille Yuvarajin [2016] suorittamassa kyselyssä Librarika-kirjastojärjestelmän käytössä. Librarika on pilvipohjainen kirjastojärjestelmä, joka sisältää kirjastojärjestelmän oleellisimmat moduulit. Yuvaraj [2016] arvioi Librarikan käyttöä "Central University of South Bihar" akateemisessa kirjastossa. Arvioinnissa hän on suorittanut kyselyn kirjastoammattilasilla, jossa on kysytty Librarikan käyttökokemuksista, sen hyötyjä ja ongelmakohtia, sekä mitä parannuksia he haluaisivat siihen. Kyselyn perusteella hän arvioi, että yksi suurimmista Librarikan käytön ongelmakohdista on tiedon omistajuus. Tähän liittyen kyselystä ilmenee, että kirjastoammattilaisten suurin toive Librarikaan lisättävistä ominaisuuksista on tiedon siirrettävyys.

Näkemykseni mukaan Yuvarajin [2016] tekstistä käy ilmi, että tietoturvallisuuteen liittyvät uhat ovat keskeinen syy, miksi kirjastot eivät tunne pilvipalveluita turvallisiksi. Tiedon omistajuuden menettäminen tarkoittaa, että tiedon eheys ja saatavuus ovat vaarassa. Samoin tiedon siirrettävyys on nähtävissä osana tätä menetystä, koska ei voida olla enää siirrettäessä varmoja, että tiedosta ei jää luvattomia kopioita tai että se on ylipäätänsä mahdollista.

Yuvaraj [2015] on tutkielmassaan havainnut tiedon omistajuuden yhtenä tietoturvahaasteena pilvipalveluja hyödyntävissä kirjastoissa. Tutkielmassaan hän suoritti kyselyn Bahar Hindu yliopiston kirjastotyöntekijöillä. Kyselyssä hän pyrki selvittämään kirjastoammattilaisten asenteita pilvipalveluja kohtaan. Tavoitteena hänellä oli saada tietää, mitkä ovat avainasiat, jotta pilvipalvelujen käyttöönotto on otollista.

Yuvarajin [2015] kyselyyn vastanneista yli puolet olivat sitä mieltä, että esteenä pilvipalvelujen käyttöönotossa on epävarmuus kirjaston ulkopuolisiin palvelimiin tallennetun tiedon turvallisuudesta. Tämän lisäksi tiedon siirrettävyys oli huolenaiheena kyselyyn vastanneilla. Hän tulkitsee, että pilvipalveluiden käyttö tarkoit-

taa, että kirjasto menettää hallinnan tiedostaan. Hän arvioi, että siirrettävyys palvelussa tai palvelusta kokonaan pois, on yksi suurimmista pilvipalvelujen käyttöönoton esteistä kirjastoissa.

Yuvarajin [2015] kyselystä voidaan tehdä johtopäätös, että kirjastoammattilaisten huolenaiheena pilvipalveluiden käyttöönotossa on kirjaston tietoturvallisuuden heikkeneminen. Näkemykseni mukaan kyselystä käy ilmi, että kirjaston pilvipalveluihin tallennetun tiedon saatavuus ja eheys tulevat olemaan vaarassa. Kirjasto ei voi olla varma, mitä tiedolle tapahtuu ja kuinka sitä käsitellään, jos se annetaan kirjaston ulkopuolisen tahon alaisuuteen.

Mavodza [2013] on havainnut omassa tutkielmassaan tiedon omistajuuden yhtenä tietoturvauhkana kirjastojen pilvipalveluiden käytössä. Tutkielmassaan hän käy läpi pilvipalvelujen vaikutusta akateemisiin kirjastoihin. Hän arvioi tekstissään, että hallinnan menetys pilvipalveluun tallennetusta tiedosta on yksi asia, joka huolestuttaa käyttäjiä pilvipalveluiden käytössä. Vastaavasti hän näkee, että useilla käyttäjillä on pelkoja tiedon omistajuuden menettämisestä. Tutkielmasta voidaan päätellä, että tietoturvallisuuden merkittävänä uhkatekijänä on tiedon omistajuuden menettäminen pilvipalveluiden käytössä. Pilvipalveluiden käyttöönotto kirjastojärjestelmissä on vaativaa, koska ne ovat uhka kirjaston tiedon saatavuudelle ja eheydelle.

Tiedon omistajuuden menettäminen voi ilmetä tiedon siirtämisen vaikeutena pilvipalvelusta pois. Fox [2009] näkee tällaisen tilanteen tapahtuvan, jos pilvipalvelun toimittaja lopettaa toimintansa. Hän kyseenalaistaa kuinka helppoa tällaisessa tapauksessa mahdollisesti on siirtää tallennetut tiedot toiselle pilvipalvelulle. Näkemykseni mukaan tiedon siirrettävyyteen liittyy kysymyksiä tiedon kopioitumisesta ja tuhoamisesta. Jos tieto siirretään pilvipalvelusta pois, jääkö siitä mahdollisesti haluttomia kopioita. Sama tilanne voi toteutua, kun tietoa määrätään tuhottavaksi. Tiedon siirrettävyyteen tilanteessa, jossa kirjasto on menettänyt tiedon omistajuuden, voidaan nähdä tiedon eheyteen liittyviä uhkia.

Wang ja muut [2011] väittävät, että keskustelu pilvipalveluiden tiedon omistajuudesta on ollut tärkeä aihe viime aikoina. Artikkelissaan he tutkivat pilvipalvelujen vaikutuksia kirjastoille. He väittävät, että pilvipalveluiden käyttö millä tahansa kirjaston osa-alueella tarkoittaa, että kirjasto ei omaa hallintaa tiedoistaan. Tämän seurauksena he näkevät, että tiedon omistajuuden menettämisellä on vaikutus yksityisyyteen. Voidaan tehdä johtopäätös, että pilvipalveluihin tallennetun tiedonhallinnan menetys johtaa kaikkien kolmen tietoturvatekijän menettämiseen. Tiedon omistajuuden menettäminen on uhka sekä tiedon eheydelle ja saatavuudelle että luottamuksellisuudelle.

3.2 Yksityisyys

Pilvipalveluissa yksityisyydellä tarkoitetaan muun muassa, että sinne tallennettua tietoa pääsevät tarkastelemaan, käyttämään ja muokkaamaan vain siihen käyttöluvan omaavat henkilöt. Yksityisyyteen liittyvät uhkatekijät voivat kohdistua jo esimerkiksi verkkokirjastoa käytettäessä, jolloin rekisteröidystä käyttäjästä kerätään tietoa hänen toiminnoistaan järjestelmässä.

Wang ja muut [2011] näkevät, että yksityisyyshuolet syntyvät tiedon omistajuuden menetyksestä pilvipalveluissa. He arvioivat, että kirjaston käyttäjätiedot, kuten asiakkaiden ja henkilökunnan tiedot, voivat mahdollisesti tulla julkisiksi. Kirjasto ei enää omaa hallintaa omasta tiedostaan.

Tästä voidaan päätellä, että pilvipalveluiden käyttö kirjastoissa vaarantaa sekä asiakkaiden että henkilökunnan henkilötiedot. Tämän voidaan nähdä johtuvan tiedon luottamuksellisuuden vaarantumisella, kun kirjasto on menettänyt omistajuuden tiedosta, tallentaessaan sen pilvipalveluun. Tällöin kirjaston ulkopuolisilla mahdollisesti luvattomilla henkilöillä on mahdollisuus päästä käsittelemään tietoja.

Tiedonhallinnan menettäminen on esillä Ifijehin [2014] artikkelissa. Hän pyrkii selvittämään tekstissään, miten pilvipalveluja ja muita digitaalisia metodeja voidaan hyödyntää tutkielmien säilönnässä, Nigerian akateemisissa kirjastoissa. Tutkielmassaan hän tulkitsee, että tietomurrot ovat mahdollinen tietoturvauhka pilvipalveluiden käytössä. Hän näkee, että kirjasto voi menettää hallinnan tiedoistaan, ulkopuolisten tai sisäisten tahojen yhteisen juonittelun seurauksena. Tähän liittyen hän arvioi, että mahdollinen tietoturvariski syntyy, jos pilvipalveluihin tallennettuihin tietoihin pääsee käsiksi muita kuin käyttöluvan saaneet henkilöt. Yksityisyyteen liittyvät tiedot voivat vaarantua.

Ifijehin [2014] tekstistä on mahdollista päätellä, että kirjaston ulkopuolinen toimija, kuten pilvipalvelun toimittaja, on tietoturvallinen uhkatekijä. Tiedon luottamuksellisuus ei toteudu, jos sitä pääsee käyttämään tai tarkastelemaan luvattomat henkilöt. Näkemykseni mukaan ei riitä, että kirjastojen pilvipalveluihin tallennettujen tietojen pääsynhallintaa valvotaan, koska käyttöluvan saanut henkilö voi mahdollisesti väärinkäyttää henkilötietoja ulkopuolisten tahojen kanssa.

Ulkopuolisista tahoista muodostuvaa tietoturvariskiä yksityisyydelle ovat arvioineet Erturk ja muut [2015]. He tarkastelevat tutkielmassaan SaaS-palvelutyyppistä EzProxy-ohjelmaa. EzProxy on kirjastojen käyttämä ohjelmisto, jonka toimittajana on OCLC niminen yritys. Siitä on olemassa sekä paikallisesti ylläpidettävä että pilvipohjainen versio, joista jälkimmäistä tarkastellaan tutkielmassa. Sitä käytetään, kun käyttäjä haluaa käyttää kirjaston hankkimia tietokantoja, yliopistokampuksen ulkopuolelta.

Erturk ja muut [2015] arvioivat, että tapa, jolla käyttäjä muodostaa yhteyden kirjaston tietokantoihin EzProxyn avulla, on uhkatekijä käyttäjän yksityisyydelle. Käyttäjän todentaminen tapahtuu pilvipohjaisessa versiossa EzProxy-ohjelmasta, muodostamalla yhteys tietokantoihin käyttäen kirjaston AD/LDP-palvelinta, joka on käyttäjätiedot omaava tietokanta, ja OCLC:n palvelinta. Tässä Erturk ja muut [2015] näkevät tietoturvahyökkäyksen mahdollisuuden, jota kutsutaan nimellä *mies välissä* -hyökkäys (engl. man-in-the-middle attack).

Mies välissä -hyökkäyksessä käyttäjän ja palvelimen kommunikaatioon tunkeutuu ulkopuolinen hyökkääjä, jonka läsnäoloa kumpikaan keskenään kommunikoiva osapuoli ei huomaa [Norton, 2019]. Tunkeutujan läsnäolo muodostaa uhan yksityisyydelle, koska hän voi päästä käsiksi arkaluontoiseen tietoon, kuten sähköposteihin tai henkilötietoihin.

Erturkin ja muiden [2015] tekstistä on pääteltävissä, että kirjaston pilvipalveluun tallennetun tiedon luottamuksellisuus ei ole pelkästään näkyvien tekijöiden takia vaarassa. Tiedon luottamuksellisuus voi vaarantua näkymättömästi hyökkäävän tahon puolesta. Tietoon ei kohdistu ainoastaan pilvipalvelun toimittajaan liittyviä luottamushuolia tiedonkäsittelystä, vaan tietoturvahyökkäyksiä, jotka vaarantavat pilvipalveluun tallennetun tiedon.

Henkilötiedot ovat huoli Mavodzan [2013] tutkielmassa. Hän on tulkinnut tekstissään, että pilvipalvelut omaavat tietoturvariskejä yksityisyydelle. Hän arvioi, että kirjaston asiakkaiden tiedot ovat asia, joka lisää huolia luottaa pilvipalveluun tallennettuun tietoon. Tutkielmasta voidaan päätellä, että pilvipalveluun tallennetun tiedon luottamuksellisuus on uhattuna, koska kirjastoammattilaisille ei ole annettu selkeää tietoa, ketkä pääsevät kyseisiä tietoja käyttämään ja tarkastelemaan. Tästä voidaan tehdä johtopäätös, että kyseinen uhka syntyy, koska tiedot eivät pilvipalvelussa enää sijaitsisi kirjaston sisällä. Tästä on pääteltävissä, että kirjastoammattilaiset kokevat, että heillä on mittavampi hallinta tiedosta, jos se sijaitsee kirjaston omissa tiloissa.

Wang [2014] vastaavasti näkee, että pilvipalvelun toimittaja itse on uhkatekijä yksityisyydelle. Tutkielmassaan hän on arvioinut pilvipalvelujen tuomia muutoksia kirjastojärjestelmiin. Hän väittää, että pilvipalveluita voidaan kirjastoihin mahdollisesti toimittaa yhdeltä pilvipalvelulta, jolla on tämän lisäksi itsellään pilvipalveluita, jotka toimittavat esimerkiksi tallennus- ja laskentakapasiteettia. Nämä pilvipalvelut ovat Wangin [2014] mukaan näkymättömiä. Ne voivat mahdollisesti päästä, kirjaston tietämättä, lukemaan tallennettuja tietoja.

Wangin [2014] väitteistä voidaan tehdä johtopäätös, että kirjastojen tietojen yksityisyys ei ole uhattuna vain yksittäiseltä kirjaston ulkopuoliselta toimijalta tai tietoturvahyökkäykseltä. Sen sijaan tietojen luottamuksellisuus voi olla vaarassa

näkymättömältä pilvipalvelun alitoimittajalta. Kirjaston ei ole välttämättä edes mahdollista huomata luottamuksellisuuden vaarantumista, jolloin ei tiedetä, minkä tietojen ja minä ajanjaksona yksityisyyttä on rikottu.

Näkymätön käyttäjien tietojen tarkkailu on Kritikosin ja muiden [2017] tutkielman keskiössä. He ovat tekstissään selvittäneet pilvipohjaisten hakuliittymien tuomia uhkatekijöitä kirjaston yksityisyyteen ja toimintaan. Tätä he ovat tutkineet käytännössä, arvioimalla BiblioCommons-hakuliittymää.

Tuloksena Kritikos ja muut [2017] ovat saaneet, että BiblioCommons-hakuliittymän toimiminen edellyttää, että se kerää tietoja kirjaston käyttäjien toiminnoista. Tämä tapahtuu seuraamalla käyttäjän toimintaa, hakuliittymän käytössä, esimerkiksi verkkoselaimen evästeiden avulla. Kritikos ja muut [2017] näkevät, että tämä muodostaa ongelman kirjastoille, koska heillä on pitkät perinteet yksityisyyden vaalimisesta. He suosittelevat, että kirjastot päivittävät tietosuojaselosteensa kertomaan, että mitä tietoja kerätään ja miten niitä käsitellään.

Tutkielmasta on mahdollista tehdä johtopäätös, että evästeiden avulla voidaan kerätä henkilötietoihin verrattavat tiedot. Tällöin tiedon luottamuksellisuus on uhattuna, koska ei voida olla varmoja ketkä pääsevät käsittelemään evästeistä kerättyjä tietoja. Suomessa ja muissa Euroopan Unionin maissa tätä uhkaa lievittää se, että evästeistä on kerrottava ja käsiteltävä EU:n tietosuoja-asetuksen mukaisesti [EU 2016/679, 2016].

Kaushik ja muut [2013] tekemässään kyselyssä ovat havainneet, että kirjastoammattilaisille tärkein asia pilvipalveluiden valinnassa on tietosuojaseloste. Heidän kyselynsä on pyrkinyt selvittämään kirjastoammattilaisten asenteita pilvipalveluja kohtaan. Tuloksena on saatu, että suurimpia esteitä pilvipalvelujen käyttöönotolle kirjastoissa ovat turvallisuus, luotettavuus ja lailliset ongelmat. Jälkimmäisestä voidaan nähdä, miksi tietosuojaseloste on tärkeä kirjastoammattilaisille. Näkemykseni mukaan tästä voidaan tehdä johtopäätös, että kirjastoammattilaiset kokevat tiedon luottamuksellisuuden olevan uhattuna, jos otetaan käyttöön pilvipalveluja kirjastojärjestelmään.

Trittin ja muiden [2014] kysely antaa kuvan, että luottamus pilvipalveluun ja siitä syntyvät yksityisyyshuolet ovat merkittävin käyttöönoton este pilvipalveluille kirjastoissa. Kyselyn vastanneet ilmaisivat, että heillä ei ole luottamusta tallentaa arkaluontoista tietoa pilvipalveluun, jotta sitä eivät muut pääse käyttämään. Samoin vastaajat kokivat, että yksityisyys luo epävarmuutta pilvipalvelujen käyttöönottoon kirjastoissa. Näkemykseni mukaan tiedon luottamuksellisuus on yksi tietoturvallinen tekijä, joka on kirjastoammattilaisten mukaan uhattuna, pilvipalveluita käyttäessä. Tekstistä on pääteltävissä, että huolet luvattomasta pääsystä kirjaston tietoihin ovat este niiden käyttöönotolle.

Fox [2009] mainitsee tekstissään samanlaisen luottamuksen puutteen yhtenä huolenaiheena pilvipalvelujen käytössä kirjastoissa. Tutkielmassaan hän käy läpi hyötyjä ja haasteita, joita pilvipalvelujen käytössä kirjastojärjestelmissä voi ilmetä. Hän arvioi, että vaikka pilvipalvelun kanssa olisi tehty hyvin selkeä ja tehokas palvelutasosopimus on silti tietoja, joita kirjasto haluaa pitää omilla palvelimillaan. Samoin hän näkee, että käyttäjillä tulee kaikesta huolimatta olemaan huolia heidän tietojen yksityisyydestä pilvipalveluissa. Voidaan tehdä johtopäätös, että kirjastojen henkilökunta on epäileväinen, säilyykö pilvipalveluun tallennetun tiedon käyttöoikeudet samana kuin mitä ne ovat kirjaston sisällä. Tästä voidaan päätellä, että tiedon luottamuksellisuus vaarantuu, jos kirjastojen tieto siirtyy pilvipalveluun.

Kirjallisuuskatsauksen tehneet Stukalova ja muut [2016] ovat sitä mieltä, että pilvipalveluiden käyttöön liittyy huolia yksityisyydestä. He arvioivat, että suurimmat huolet pilvipalvelujen käytössä ovat turvallisuus ja yksityisyys. He väittävät, että kirjastoilla ei tästä ole huolta, koska niillä ei ole arkaluontoisia tietoja. Näkemykseni mukaan tämä väite ei kuitenkaan pidä paikkaansa Suomessa, koska kirjastokortin saa vain, jos luovuttaa kirjastolle omat henkilötiedot [PIKI-verkkokirjasto asiointi, 2019; Helmet-kirjastot, 2018]. Tästä voidaan päätellä, että suomalaisilla kirjastoilla on samat huolet yksityisyydestä kuin muilla arkaluontoisia tietoja omaavilla pilvipalvelujen käyttäjillä.

Yuvaraj [2015] näkee, että yksityisyys on yksi tärkeimmistä huolenaiheista, joita kirjastoilla on pilvipalveluja kohtaan. Heidän kyselyn tuloksena kahdeksan prosenttia kirjastoammattilaisista koki yksityisyyden olevan esteenä pilvipalvelujen käyttöönotolle. Tästä voidaan tehdä johtopäätös, että pilvipalvelun koetaan olevan uhkatekijä tiedon luottamuksellisuudelle, jolloin se on uhka yksityisyydelle.

Vastaavasti Yuvarajin [2016] suorittamassa kyselyssä yksityisyyden koki yli kahdeksankymmentä prosenttia vastaajista alueeksi, jota tulisi parantaa Librarika-kirjastojärjestelmässä. Samoin yli seitsemänkymmentä prosenttia vastaajista kertoi, että yksityisyys oli yksi ongelmista, joita he olivat kohdanneet Librarikan käytössä. Tästä voidaan päätellä, että Librarika-kirjastojärjestelmän käsittelemän tiedon ei koeta olevan vain luvan saaneiden henkilöiden käytettävänä. Tällöin kirjastojärjestelmä vaarantaa tiedon luottamuksellisuuden.

3.3 Datakeskuksen sijainti

Tiedon omistajuuteen ja yksityisyyteen liittyvät tietoturva- ja tietosuojauhat on mahdollista ratkaista linjauksilla, asetuksilla, standardoinnilla ja lailla [Yuvaraj, 2016; Yuvaraj, 2015]. Näitä voivat määritellä sekä kirjasto itse että esimerkiksi maan hallitus tai jäsenvaltioista koostuva liittouma kuten Euroopan Unioni. Nämä

eivät välttämättä tarjoa täydellistä ratkaisua, koska pilvipalveluihin tallennettu tieto voi olla sijoitettu datakeskukseen, joka sijaitsee eri maassa tai maanosassa kuin missä pilvipalvelun käyttäjä on. Pilvipalveluun tallennetun tiedon ei voida olettaa olevan samojen lakien ja asetusten alainen kuin pilvipalvelun käyttäjä on. Suomessa Euroopan Union tietosuoja-asetuksen tulisi tämä osittain turvata. Asetus ei kuitenkaan kiellä tietojen siirtämistä Euroopan Unionin ulkopuolelle, mutta sen artiklat 44-50 pyrkivät takaamaan, että niitä käsitellään tällaisissa tilanteissa tietosuoja-asetuksen mukaisesti [EU 2016/679, 2016]. Lähdekirjallisuus ei ole keskittynyt Suomeen, joten datakeskuksen sijainnista syntyvät tietoturvauhat ovat nousseet ilmi. Tästä on nähty, että ne ovat yksi mahdollinen tietoturvauhkatekijä pilvipalveluja hyödyntäville kirjastojärjestelmille.

Goldner [2010] on nostanut datakeskuksen sijainnin yhdeksi tietoturvalliseksi vaaran tekijäksi kirjastojen pilvipalveluiden hyödyntämisessä. Hän arvioi, että kirjaston saada tietää, missä pilvipalveluun tallennetun tiedon omaava datakeskus sijaitsee, jotta voidaan varmistaa, että datakeskus on samojen tietosuojalakien alainen kuin kirjasto. Tekstistä voidaan päätellä, että kirjastojen tiedon sijaitseminen kirjaston ulkopuolella aiheuttaa epäselvyyttä, mitä lakeja pilvipalveluun tallennettuun tietoon sovelletaan. Lakien ei voida olettaa suojaavan tietoa, jolloin siihen voi kohdistua uhkia, jotka vaarantavat tiedon eheyden, luottamuksellisuuden ja saatavuuden.

Abidi ja muut [2011] ovat tarkastelleet pilvipalvelun luomia mahdollisuuksia kirjastoille. He ovat yleisesti positiivisia pilvipalvelujen tuomista hyödyistä ja näkevät, että kaikki ongelmat ovat helposti ratkaistavissa. Tästä huolimatta he huomauttavat, että kirjastojen tulee vaatia pilvipalveluja hankkiessaan datakeskuksen sijainti. Näin siksi, että pystytään luomaan luottamuksellinen suhde pilvipalvelun toimittajan kanssa, jota normaalisti ei ole. Tästä voidaan tehdä johtopäätös, että pilvipalvelut koetaan oletuksena epäluotettaviksi. Vain lait, asetukset ja linjaukset auttavat lieventämään tätä tunnetta. Tällöin pystytään varmistamaan tietoturvallisuus pilvipalvelua käytettäessä.

Luottamuksen puute pilvipalvelun toimittajaan on esillä Wangin ja muiden [2011] tutkielmassa. He arvioivat, että kirjaston ulkopuolelle tallennettuun tietoon liittyy sekä turvallisuushuolia että laillisia ongelmia. He näkevät, että ulkopuolisen tiloihin tallennettu tieto luo turvattomuuden tunnetta.

Näkemykseni mukaan, kun kirjaston tieto ei sijaitse kirjaston tiloissa, aiheutuu huolia tietoturvallisuudesta. Tämän voidaan päätellä ilmenevän siitä, että jos tieto ei sijaitse kirjaston tiloissa ei välttämättä tiedetä missä se sijaitsee. Ei voida olla varmoja, että se on samojen lakien ja asetuksien alainen, joilla tietoturvallisuus varmistettaisiin.

Kirjaston ulkopuolelle tallennetun tiedon turvallisuushuolet ilmenevät Yuvarajin [2016] teettämässä kyselyssä. Kyselyn vastaajat ilmaisivat, että yhtenä Librarika-kirjastojärjestelmän ongelmakohtana on datakeskuksen sijainti. Tämä turvallisuusuhka oli kuudenneksi suurin huoli, jota yli seitsemänkymmentä prosenttia vastaajista piti merkittävänä ongelmana. Tähän liittyen kyselyn vastaajat kertoivat, että toiseksi tärkein parannuskohde on sääntöjen määrittäminen, jota yli yhdeksänkymmentä prosenttia piti tärkeimpänä. Tästä voidaan tehdä johtopäätös, että datakeskukseen tallennetun tiedon tulisi olla samojen sääntöjen, linjauksien, lakien ja asetusten alainen kuin kirjasto itse, vaikka tieto ei enää sijaitse kirjaston omissa tiloissa.

Sääntöjen ja linjauksien määrittäminen on esillä Makorin [2016] tutkielmassa. Hän nostaa esille, että tallennettu tieto voi pilvipalveluissa sijaita toisessa maassa kuin kirjasto. Hänen mukaansa on tärkeää määrittää säännöt, joita noudatetaan yli maiden rajojen. Tästä voidaan päätellä, että linjaukset, joiden alainen kirjasto on, ei välttämättä sovelleta pilvipalveluun. Voidaan nähdä syntyvän ristiriita, koska tietoa käsiteltäisiin tällöin eri sääntöjen alaisuudessa kuin miten kirjasto niitä käsittelee. Tämän voidaan päätellä olevan tietoturvariski, koska säännöt, jotka varmistaisivat tiedon turvallisuuden, eivät enää koskisi pilvipalveluun tallennettua tietoa.

Stukalova ja muut [2016] ovat tekemässään kirjallisuuskatsauksessaan tulkinneet, että pilvipalvelut eivät välttämättä sijaitse yhdessä tietyssä maassa. Pilveen tallennettuun tietoon tullaan soveltamaan eri lakeja. Esimerkkinä he nostavat Yhdysvaltojen terrorisminvastaiset lait, joita sovelletaan eri tavoin muihin maihin.

Tekstissään Stukalova ja muut [2016] eivät tarkenna, mitä lakia he tarkoittavat. Voidaan olettaa, että Yhdysvaltojen terrorisminvastaisella lailla he viittaavat niin sanottuun Patriot Act -lakiin. Laki laajensi Yhdysvaltojen viranomaisten oikeuksia saada haltuunsa tietoja, joita Yhdysvallat kokevat olevan yhteyksissä terrorismitoimintaan [USA Patriot Act, 2001]. Pilvipalvelu, jonka datakeskus sijaitsisi Yhdysvalloissa, tulisi olemaan kyseisen lain säätelemä.

Stukalova ja muut [2016] näkevät, että pilvipalveluiden toimittaminen verkon kautta, estää oletuksena niiden datakeskuksen sijainnin tietämisen. Esimerkiksi turvallisuusauditointien tekeminen ja varmistaminen on tällöin haastavaa. Tekstistä voidaan tehdä johtopäätös, että datakeskuksen sijainnin tietäminen vaikuttaa tietoturvan laatuun. Tämä voidaan päätellä siitä, että datakeskuksen sijainnin tietäminen varmistaa, onko se samojen lakien ja asetusten alainen kuin kirjasto.

4 Pohdinta

Lähdekirjallisuuden perusteella on saatu tulokseksi, että kirjastoilla on useita tietoturvahuolia pilvipalveluiden käytöstä. Näitä ovat tiedon omistajuus, yksityisyys ja datakeskuksen sijainti, jotka ovat liitettävissä tietoturvatekijöiden ja tietosuojan vaarantumiseen. Näiden yhteisenä tekijänä voidaan nähdä pilvipalvelun toimittaja, johon kohdistuva epäluottamus mahdollistaa nämä tietoturva- ja tietosuojauhat.

Näkemykseni mukaan tällaisessa tapauksessa, jossa luottamuksen puute on pitkälti esteenä pilvipalveluiden käytölle, tulisi panostaa yhteisiin sääntöihin. Esimerkiksi palvelutasosopimuksen teko tulisi luomaan luottamuksellisen suhteen kirjaston ja pilvipalvelun toimittajan välille. Siinä voitaisiin määritellä sekä yhteiset tietoturva- ja tietosuojalinjaukset että sanktiot, jos niitä rikotaan. Tämä linjauksien määrittäminen on nähtävissä lähdekirjallisuudessa yhtenä ratkaisuna [Kaushik, 2013; Yuvaraj, 2016].

Lähdekirjallisuudesta on huomioitava ensiksi se, että ne ovat pitkälti samoilla linjoilla asioista. Kaikki ovat nähneet vähintään yhden löydetyistä tietoturvahaasteista kohtana, joka kirjaston tulee ottaa huomioon pilvipalveluja hankkiessa. Tästä voidaan päätellä, että kyseiset tietoturvahaasteet ovat pitkälti jo tiedossa. Ne eivät ole pelkästään kirjaston haasteita, vaan yleisesti pilvipalveluihin liittyviä tietoturvaongelmia. Tutkielma ei sinänsä tuo uutta tietoa näistä uhista. Sen sijaan se antaa yleisen katsauksen, miten ne ilmenevät kirjastojen näkökulmasta.

Syytä on huomioida, että lähdekirjallisuudesta ilmenevät tutkija- ja tutkimusmaat ovat pitkälti Euroopan ulkopuolisia. Saatuja tuloksia ei sellaisenaan voida yleistää Suomen kirjastoihin EU:n tietosuoja-asetuksen takia. Esimerkiksi datakeskuksen sijainnista syntyvät luottamushuolet vähenevät EU:n tietosuoja-asetuksen takia. Voidaan nähdä, että tutkielma olisi ollut kannattavampi kirjoittaa englannin kielellä. Tällöin se olisi ollut saatavilla kansainvälisemmälle yleisölle, jota tässä löydetyt tietoturva- ja tietosuojauhat ehkä enemmän koskettavat. Tästä huolimatta tuloksena on saatu näkemys tietoturvahaasteista, joita ilmenee pilvipalveluita hyödyntävissä kirjastojärjestelmissä.

Itse kirjastojärjestelmä-termin käytöstä voidaan huomioida sen vastaavuus kirjasto-termin kanssa. Näkemykseni mukaan kirjastojärjestelmän sijaan olisi ollut mahdollista puhua pelkästä kirjastosta. Kirjastojärjestelmä on se järjestelmä, jonka avulla kirjasto toteuttaa toimiaan. Kirjasto ja kirjastojärjestelmä ovat riippuvaisia toistensa olemassaolosta. Voidaan päätellä, että niitä on mahdollista tässä kontekstissa käsitellä synonyymeinä.

Synonyymisuus kirjastojärjestelmä- ja kirjasto-termien välillä oli nähtävissä valikoidessa kirjallisuutta. Näkemykseni mukaan eri englannin kielisten kirjastojärjestelmä-termien käyttö oli aineiston löytämisen kannalta hyödytöntä. Usein hauissa saatiin tuloksia, joissa kyllä mainittiin esimerkiksi "integrated library system", mutta siihen viitattiin itse tekstissä "library"-sanalla. Hakulausekkeita tehdessä olisi voitu käyttää kyseistä sanaa korvaamaan eri englannin kieliset kirjastojärjestelmä sanat. Väittäisin että tällöin olisi saatu lähes samat tulokset kuin nyt. Näkemykseni mukaan muulta osin hakulausekkeet olivat onnistuneita ja ne tuottivat aineistoa, joka tarjosi vastauksen tutkimusongelmaan.

Tuloksien pohjalta voitaisiin lähteä tekemään jatkotutkimusta, jossa pyrittäisiin selvittämään, miten kirjastot ja pilvipalveluiden toimittajat varmistavat luottamuksen toisiinsa. Tapahtuuko se esimerkiksi palvelutasosopimusten avulla? Tätä tulisi tutkia, koska lähdekirjallisuus pitkälti toisti samoja tietoturvahaasteita. Tästä voidaan päätellä, että niiden tulisi olla yleisesti tiedettyjä haasteita pilvipalvelujen käyttöönotossa. Pilvipalveluja hankkiessa tulisi jo olla tiedossa nämä uhat sekä, miten niihin tulisi varautua.

Lähdekirjallisuudessa esiintyvät tutkimukset on pitkälti suoritettu Euroopan ulkopuolella. Olisi hyödyllistä selvittää pilvipalveluiden käyttöönottoaste esimerkiksi Suomen kirjastoissa. Samalla tulisi selvittää, minkälaisia tietoturvaan liittyviä ongelmia niiden mahdollisessa käyttöönotossa on ilmennyt. Erityisesti tulisi tarkastella Euroopan Unionin tietosuoja-asetuksen tuomia vaikutuksia. Näitä tulisi tarkastella erityisesti datakeskuksen sijainnista syntyvien tietosuojaongelmien näkökulmasta. Esimerkiksi, onko tietosuoja-asetus auttanut turvaamaan pilvipalveluun tallennetut tiedot, kun datakeskus sijaitsee Euroopan ulkopuolella.

Näkemykseni mukaan tulisi tutkia tietoturva- ja tietosuojahaasteita pilvipalveluita hyödyntävissä kirjastojärjestelmissä, erään tässä tutkielmassa esitellyn rajoituksen näkökulmasta. Minkälaisia vaikutuksia avoimella ja suljetulla lähdekoodilla on? Esimerkiksi, onko sillä vaikutusta tietoturvaan, jos kirjastojärjestelmä on avoimen lähdekoodin alainen, mutta pilvipalvelu on toteutettu suljetulla lähdekoodilla?

Lisäksi olisi hyödyllistä tutkia, miten pilvityyppi vaikuttaa tietoturvallisuuteen. Yksityinen pilvi olisi mahdollisesti turvallisempi, mutta aiheuttaako se lisää kuluja, mikä vähentäisi pilvipalvelujen keskeisintä hyötyä kirjastoille eli kustannustehokkuutta. Entä voisiko yhteisöllinen pilvi antaa kirjastoille, jotka ovat päättäneet käyttää samaa pilvipalvelua, vaikutusvaltaa pilvipalvelun toimittajaan, jotta tämä panostaa tietoturvallisuuteen. Hybridipilveä tulisi tarkastella, koska kirjastojen aineistoviitetietokanta ei välttämättä niin tärkeä tietoturvallisuuden näkökulmasta

kuin asiakkaiden ja henkilökunnan henkilötiedot. Voitaisiin käyttää julkista pilvityyppiä viitetietokannan tallentamiseen ja yksityistä pilveä henkilötietojen turvallisuuden varmistamiseen.

5 Yhteenveto

Pilvipalvelut ovat huomioimisen arvoinen ratkaisu, vähäisten resurssien kanssa toimiville kirjastoille. Syynä on pilvipalveluiden kustannustehokkuus. Toisaalta pilvipalvelut ovat uutisissa niihin liittyvistä tietoturvaongelmista. Tutkielmassa on pyritty selvittämään mahdollisia tietoturva- ja tietosuojauhkia, joita voi ilmetä pilvipalveluja hyödyntävissä kirjastojärjestelmissä. Näiden selvittämiseksi on suoritettu kirjallisuuskatsaus, jossa valikoitu lähdekirjallisuus käsittelee pitkälti Euroopan ulkopuolella olevien kirjastojen pilvipalveluiden hyödyntämistä.

Kirjallisuuden perusteella on tunnistettu kolme toistuvasti ilmenevää tietoturva- ja tietosuojauhkaa. Nämä ovat tiedon omistajuus, yksityisyys ja datakeskuksen sijainti, jotka voidaan liittää eri tietoturvatekijöiden ja tietosuojan uhkatekijöiksi. Tiedon omistajuus vaarantaa sen saatavuuden ja eheyden, yksityisyys on uhkana tiedon luottamuksellisuudelle ja datakeskuksen sijainti aiheuttaa epävarmuutta tietosuojan lakien ja asetusten noudattamisesta. Näiden uhkatekijöiden yhteinen tekijä on pilvipalvelun toimittaja. Näkemykseni mukaan pilvipalveluiden käyttöönotto kirjastoissa edellyttäisi palvelutasosopimuksen tekoa, kirjaston ja pilvipalvelun toimittajan välillä. Tällaisessa sopimuksessa tulisi tarkasti määritellä, miten tietoturva ja tietosuoja varmistetaan osapuolien välillä.

Viiteluettelo

Abidi, F., Abidi, H. J. ja Armani, S. (2012). Cloud libraries: A novel application of cloud computing. *International Conference on Education and e-Learning Innovations*, Sousse, Tunisia, July 1-3, 2012. 4 sivua.

Axiell Arena (2019). Axiell Arena – Axiell Finland. https://www.axiell.fi/axiell-arena/ Haettu 23.10.2019.

Axiell Aurora (2019). Axiell Aurora – Axiell Finland. https://www.axiell.fi/tuotteet_palvelut/aurora/ Haettu 19.10.2019.

Erturk, E. ja Iles, R. (2015). Case study on cloud based library software as a service: Evaluating Ezproxy. *Journal of Emerging Trends in Computing and Information Sciences*, 6(10): 545-549.

EU 2016/679 (2016). Euroopan unionin yleinen tietosuoja-asetus 27.4. 2016/679. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX:32016R0679 Haettu 20.10.2019.

Fox, R. (2009). Library in the clouds. *OCLC Systems & Services: International digital library perspectives,* 25(3): 156-161. https://doi-org.libproxy.tuni.fi/10.1108/10650750910982539

Fu, P. ja Fitzgerald, M. (2013). A comparative analysis of the effect of the integrated library system on staffing models in academic libraries. *Information Technology & Libraries,* 32(3): 47-58.

Goldner, M. R. (2010). Winds of change: libraries and cloud computing. *BIBLIOTHEK Forschung und Praxis*, 34(3): 270-275. https://doi.org/10.1515/bfup.2010.042

Google Drive (2019). Etusivu. Google Drive. https://www.google.com/drive/ Haettu 21.10.2019.

Helmet-kirjastot (2018). Oma kirjastokortti. Helmet. 1.3.2018. https://www.helmet.fi/fi-FI/Lapset/Kirjastossa/Oma_kirjastokortti Haettu 21.11.2019.

Ifijeh, G. (2014). Adoption of digital preservation methods for theses in nigerian academic libraries: Applications and implications. *The Journal of Academic Librarianship*, 40(3-4): 399-404. https://doi.org/10.1016/j.acalib.2014.06.008

Ikäheimo, Ulla (2019). MARC 21 -yhtenäisformaatit. Kansalliskirjasto 03.10.2019. https://www.kiwi.fi/display/Marc21/Palvelun+kuvaus

Kaushik, A. (2013). Libraries Perception Towards Cloud Computing: A Survey. World Digital Libraries, 6(1): 13-24.

Kaushik, A. ja Kumar, A. (2013). Application of Cloud Computing in Libraries. *International Journal of Information Dissemination and Technology*, 3(4): 270-273.

Kritikos, K. C. ja Zimmer, M. (2017). Privacy Policies and Practices with Cloud-Based Services in Public Libraries: An Exploratory Case of BiblioCommons. *Journal of Intellectual Freedom and Privacy*, 2(1): 23-37. DOI:10.5860/jifp.v2i1.6252

Makori, E. O. (2016). Exploration of cloud computing practices in university libraries in Kenya. *Library Hi Tech News*, 33(9): 16-22. DOI:10.1108/LHTN-11-2015-0077

Mavodza, J. (2013). The impact of cloud computing on the future of academic library practices and services. *New Library World*, 114(3/4): 132-141. https://doi-org.libproxy.tuni.fi/10.1108/03074801311304041

Microsoft Azure (2019). Get to know Azure. Microsoft Azure. https://azure.microsoft.com/en-us/overview/ Haettu 21.10.2019.

Norton (2019). What is a man-in-the-middle-attack? NortonLifeLock. https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html Haettu 8.11.2019.

OKM (2019). Mitä tietosuoja tarkoittaa? OKM. Opetus- ja kulttuuriministeriö. https://minedu.fi/mita-tietosuoja-tarkoittaa- Haettu 20.10.2019.

Opiskelijan digitaidot (2019). Opiskelijan digitaidot. Helsingin yliopisto – orientaatio. https://blogs.helsinki.fi/opiskelijan-digitaidot/4-tietoturva/4-1-tietoturvan-ja-tietosuojan-perusteet/yksilon-tietosuoja/ Haettu 23.10.2019.

PIKI-verkkokirjasto asiointi (2019). Asiointi PIKI-kirjastoissa. https://piki.verkkokirjasto.fi/web/arena/asiointi Haettu 21.11.2019.

PIKI-verkkokirjasto ohjeet (2018). Ohjeet. Omat tiedot. PIKI-verkkokirjasto. 15.8.2018. https://piki.verkkokirjasto.fi/web/arena/ohjeet/-/asset_publisher/j8UD/content/omat-sivut-omat-tiedot?inheritRedirect=false&redirect=https%3A%2F%2Fpiki.verkkokirjasto.fi%2Fweb%2Farena%2Fohjeet%3Fp_p_id%3D101_INSTANCE_j8UD%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-1%26p_p_col_pos%3D1%26p_p_col_count%3D2 Haettu 25.11.2019.

Stukalova, A. A. ja Guskov, A. E. (2016). Publications on the use of cloud technologies at libraries. *Scientific and Technical Information Processing*, 43(1): 47-57. DOI:10.3103/S0147688216010093

Tietosuojavaltuutettu: henkilötieto (2019). Mikä on henkilötieto? Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/mika-on-henkilotieto Haettu 23.10.2019.

Tietosuojavaltuutettu: tietosuoja (2019). Mitä tietosuoja on? Tietosuojavaltuutetun toimisto. https://tietosuoja.fi/tietosuoja Haettu 23.201.2019.

Traficom (2019). Tietoturva. Kyberturvallisuuskeskus. Traficom Liikenne- ja viestintävirasto Kyberturvallisuuskeskus 02.09.2019. https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/tietoturva Haettu 20.10.2019.

Tritt, D. ja Kendrick, K. D. (2014). Impact of cloud computing on librarians at small and rural academic libraries. *The Southeastern Librarian*, 62(3): 2-11.

USA Patriot Act (2001). USA Patriot Act of 2001. H.R.3162. 23.10.2001. https://www.congress.gov/bill/107th-congress/house-bill/03162 Haettu 7.11.2019.

Wang, L. J. (2014). Cloud-Based University Library Management System, Teoksessa Wenjiang Du ja Maode Ma (Toim.), *Applied Mechanics and Materials*, vol. 484-485: pages 824-828.

Wang, X. ja Huang, J. (2011). What Cloud Computing Means to Libraries and Information Services. *Journal of Library & Information Science*, 37(2): 166-174.

Yuvaraj, M. (2015). Problems and prospects of implementing cloud computing in university libraries. *Library Review*, 64(8/9): 567-582. https://doi-org.libproxy.tuni.fi/10.1108/LR-01-2015-0007

Yuvaraj, M. (2016). Library automation with cloud based ILMS Librarika: case study of Central University of South Bihar. *Library Hi Tech News*, 33(7): 13-17. DOI:10.1108/LHTN-04-2016-0016