Jaso Ristimäki

TEKOÄLYN YLEISTYMISEN RISKIT JA HAASTEET FINANSSIALALLA

JYVÄSKYLÄN YLIOPISTO

INFORMAATIOTEKNOLOGIAN TIEDEKUNTA

2020

TIIVISTELMÄ

Ristimäki, Jaso
Tekoälyn yleistymisen riskit ja haasteet finanssialalla
Jyväskylä: Jyväskylän yliopisto, 2020, 67 s.
Tietojärjestelmätiede, pro gradu -tutkielma
Ohjaaja(t): Pulkkinen, Mirja

Tekoälyä käytetään paljon finanssialalla useissa eri yhteyksissä ja käyttö lisääntyy vuosi vuodelta. Nopeaan käytön yleistymiseen liittyy usein erilaisia haasteita tai riskejä. Finanssialan yhteiskunnallisesti tärkeän roolinsa takia ala on myös tarkoin säännöstelty ja valvottu. Tässä pro gradu tutkimuksessa tutkitaan ensiksi kirjallisuuskatsauksen pohjalta, yleisiä liiketoimintaan liittyvien riskien malleja. Katsauksessa etsitään myös vastausta siihen, millaista tekoälyä finanssialalla käytetään ja millaisia haasteita tai riskejä tekoälyyn liittyen tunnistetaan. Kansainvälisesti haasteita koettiin muun muassa työpaikkojen korvaamisessa tekoälyllä, rikollisuuden lisääntymisessä, sekä moraalisiin ja eettisiin ongelmiin liittyen. Tutkimuksen empiirisessä osuudessa tutkitaan puolistrukturoitujen haastatteluiden muodossa Suomen finanssialalla koettuja haasteita ja riskejä tekoälyn yleistyvään käyttöön liittyen. Vastauksissa korostui tekoälyn tekemät väärät tulkinnat ja päätökset, sekä oppimiseen ja kouluttamiseen liittyvät seikat. Tutkimuksen tuloksissa verrataan kirjallisuuskatsauksen tuloksia maailmalta, Suomen finanssialalta saatuihin tuloksiin, etsien yhtäläisyydet ja eroavaisuudet. Tuloksissa painotettiin riskienhallinnan tärkeyttä tekoälyyn liittyvien riskien ja haasteiden yhteydessä, joten tuloksia peilattiin myös liiketoimintaan yleisesti liittyviin riskeihin. Tutkimuksen lopussa pohditaan tutkimuksen onnistumista ja luotettavuutta, sekä mietitään mahdollisia jatkotutkimusaiheita.

Asiasanat: tekoäly, finanssiala, tekoälyn haasteet, tekoälyn riskit, tekoäly finanssialalla.

ABSTRACT

Ristimäki, Jaso
Risks and challenges of the spread of artificial intelligence in the financial sector.
Jyväskylä: University of Jyväskylä, 2020, 67 pp.
Information Systems, Master's Thesis
Supervisor(s): Pulkkinen, Mirja

Artificial intelligence is widely used in the financial sector in many different contexts and its use is increasing year by year. The rapid spread of use is often associated with various challenges or risks. Due to its socially important role in the financial sector, the sector is also tightly regulated and supervised. This master's study first examines, on the basis of a literature review, general business-related risk models. The review also seeks an answer to what kind of artificial intelligence is used in the financial sector and what kind of challenges or risks related to artificial intelligence are identified. Internationally, challenges were encountered in replacing jobs with artificial intelligence, increasing crime, and moral and ethical issues. The empirical part of the study examines the challenges and risks experienced in the Finnish financial sector in connection with the increasing use of artificial intelligence in the form of semi-structured interviews. The responses highlighted the misinterpretations and decisions made by artificial intelligence, as well as issues related to learning and training. The results of the study compare the results of the literature review with the results obtained from the world, the Finnish financial sector, looking for similarities and differences. The results emphasized the importance of risk management in connection with the risks and challenges related to artificial intelligence, so the results were also reflected in the risks related to business in general. At the end of the study, the success and reliability of the study are considered, as well as possible topics for further research.

Keywords: artificial intelligence, finance, artificial intelligence challenges, artificial intelligence risks, artificial intelligence in the financial sector.

KUVIOT

KUVIO 1 Tekoälyn tasot 14
KUVIO 2 Finanssialan veromaksut 15
KUVIO 3 Valvottavien jakauma 17
KUVIO 4 Riskiperusteinen päätöksenteko 23
KUVIO 5 Riskienhallinnan CLASS-elementit 25
KUVIO 6 Haastateltavien työvuodet 37

TAULUKOT

TAULUKKO 1 Tekoälyn yleistymisen uhat 26
TAULUKKO 2 Tekoälyn riskitasojen lajittelu 27
TAULUKKO 3 Tekoälyn haasteet ja riskit kirjallisuuskatsauksessa 29
TAULUKKO 4 Tekoälyn käyttö 39
TAULUKKO 5 Haastatteluissa todetut haasteet ja riskit 51

SISÄLLYS

TIIVISTELMÄ 2
ABSTRACT 3
KUVIOT 4
TAULUKOT 4
SISÄLLYS 5

1 JOHDANTO 7
1.1 Keskeisimmät käsitteet 8
1.1.1 Riski 8
1.1.2 Haaste 8
1.1.3 Finanssiala 8
1.1.4 FinTech 9
1.1.5 Algoritmi 9
1.2 Tutkimusongelma ja tutkimuskysymykset 9
1.3 Tutkimuksen rakenne 10

2 TEKOÄLY JA SEN SOVELTAMINEN FINANSSIALALLA 12
2.1 Tekoäly 12
2.1.1 Tekoälyn määritelmä 12
2.1.2 Tekoälyn osa-alueet ja tasot 13
2.2 Finanssiala Suomessa 15
2.2.1 Finanssialan rakenne 15
2.2.2 Finanssialan sääntely 16
2.3 Tekoäly finanssialalla 17
2.3.1 Koneoppimisen metodit 17
2.3.2 Datan louhinnan metodit 18
2.3.3 Syväoppimisen metodit 19
2.3.4 Kuvan- ja kasvojentunnistamisen metodit 19
2.3.5 Puheentunnistus, luonnollisen kielen prosessit ja robotiikka 20

3 TEKOÄLYN HAASTEET JA RISKIT FINANSSIALALLA 21
3.1 Riski liiketoiminnan yhteydessä 21
3.2 Tekoälyn haasteet ja riskit 24

3.3 Kirjallisuuskatsauksen pohdinta 28

4 EMPIIRINEN TUTKIMUS 31
4.1 Tutkimuksen taustat 31
4.2 Empiirisen tutkimuksen toteutus 32

5 EMPIIRISEN TUTKIMUKSEN TULOKSET 36
5.1 Tekoälyn rooli yrityksessä 37
5.2 Poistunut tekoäly, tulevaisuuden tekoäly ja tekoälyn hyödyt 39
5.3 Koetut haasteet ja riskit 41
5.3.1 Haasteiden ja riskien tunnistaminen 41
5.3.2 Koulutuksen ja säännöstelyn haasteet 43
5.3.3 Blackboxin riskit, sekä moraaliset ja eettiset haasteet 45
5.3.4 Palveluiden muokkaantuminen ja virheelliset tulkinnat 46
5.3.5 Tekoälyyn liittyvä rikollisuus ja vastuun jakautuminen 48
5.3.6 Suurimmat haasteet ja riskit, sekä niihin varautuminen 49

6 JOHTOPÄÄTÖKSET 51
6.1 Tulosten peilaaminen liiketoiminnan riskeihin 52
6.2 Pohdinta 54
6.3 Tutkimuksen luotettavuus 55
6.4 Jatkotutkimus 56

7 YHTEENVETO 58

LÄHTEET 60
LIITE 1 HAASTATTELUKYSYMYKSET 66

1 JOHDANTO

Tekoälyä on käytössä jo tänä päivänä todella runsaasti finanssialalla, terveydenhuollossa, teollisuudessa, itseohjautuvissa autoissa ja useilla muilla alueilla. Tekoälyn yleisimpiin hyötyihin voidaan katsoa kuuluvaksi kulujen alentuminen, toiminnan tehostaminen ja kokonaan uuden liiketoiminnan tai sen osa-alueen luominen. Tekoälyn hyödyt ovat suurimmissa osin helposti mitattavissa ja niistä on myös tehty aiempaa tutkimusta melko paljon. Tekoälyllä on valtava potentiaali muuttaa useiden alojen käytänteitä ja toimintatapoja, kuten suomalaisessa pörssiyhtiössä Tieto OYJ:ssä otettiin johtoryhmässä käyttöön tekoäly Alicia T, joka toimii johtoryhmän jäsenenä antaen neuvoja, mutta ei tee itse päätöksiä (Tieto, 2018).

Finanssiala on yksi edelläkävijäaloista tekoälyn käytön suhteen, lisäksi finanssiala on vahvasti säännelty ja valvottu sen yhteiskunnallisesti tärkeän vaikutuksen vuoksi. Tästä syystä finanssiala soveltuu hyvin tämän tutkimuksen alaksi. Uudet tekoälyohjelmistot ovat usein ensimmäisenä käytössä juuri finanssialalla. Uuden teknologian käyttöönottoon tai uuteen tapaan toimia, liittyy kuitenkin hyötyjen lisäksi myös haasteita tai suoranaisia riskejä. Tästä syystä myös tekoälyn yleistymisen mukanaan tuomia riskejä ja haasteita on syytä tutkia. Tässä tutkielmassa näitä haasteita ja riskejä tutkitaan ensiksi kirjallisuuskatsauksen pohjalta yleisellä tasolla ja pyritään löytämään maailmalta yleisimmät finanssialan tekoälyn yleistymiseen liittyvät haasteet ja riskit. Myöhemmässä osiossa tutkimusta, tekoälyn haasteita ja riskejä tutkitaan empiirisin menetelmin Suomen finanssialan yhteydessä. Empiirinen tutkimus toteutettiin puolistrukturoitujen haastatteluiden muodossa ja haastatteluihin etsittiin henkilöitä eri finanssialan yrityksistä. Tutkimusta varten saatiin haastateltua työntekijöitä kahdesta pankista, vakuutusyhtiön varainhoidosta, sekä Suomen finanssisektoria valvovasta Finanssivalvonnasta.

Tutkimuksen tuloksissa verrataan kirjallisuuskatsauksen ja empiirisen tutkimuksen tuloksia keskenään, tarkoituksena löytää yhtäläiset tekoälyn yleistymiseen liittyvät haasteet maailmalta ja Suomen finanssialalta. Pro gradu tutkimuksen loppuosiossa pohditaan syitä tutkimustuloksien samankaltaisuuksille ja eroavaisuuksille. Tulosten pohjalta voidaan todeta, että Suomessa tekoälyyn

liittyvä riskienhallinta, osaaminen ja yhteistyö eri viranomaistahojen kesken ovat avainasemassa tekoälyn haasteita ja riskejä kohdatessa.

1.1 Keskeisimmät käsitteet

Tässä luvussa esitetään tämän tutkimuksen kannalta keskeisimmät käsitteet, pois lukien tekoäly, sillä sen määritelmä käydään tarkemmin läpi luvussa 2. Osalla käsitteistä voi olla muissa yhteyksissä erilaisia määritelmiä, mutta tässä tutkielmassa näitä käsitteitä käytetään, niin kuin ne on tässä luvussa esitetty.

1.1.1 Riski

Stanfordin filosofian tietosanakirja (2017) kuvaa riskiä seuraavasti: sana ”riski” viittaa usein melko epämääräisesti tilanteisiin, joissa on mahdollista, mutta ei varmaa, että jokin ei-toivottu tapahtuma käy toteen. Riskiin liittyy siis vahvasti jokin epäsuotuisa tai ei-haluttu lopputulos. Samalla riskiin liittyy myös jokin positiivinen puoli, jota halutaan tavoitella. Haluttuun tapahtumaan tai päämäärään halutaan päästä ja riski on tämän tapahtuman tavoittelun negatiivinen toteutuminen. Riski-termiin liittyy myös todennäköisyys riskin toteutumiselle, tästä syystä riskiin liittyy, varsinkin liiketoiminnan yhteydessä riskien arviointi, sekä riskien hallinta. Näiden avulla pyritään arvioimaan ja laskemaan sitä, onko tavoiteltu tapahtuma kannattava tai järkevä suhteessa siihen liittyviin riskeihin.

1.1.2 Haaste

Cambridgen sanakirja (2020) määrittelee haasteen sellaiseksi tilanteeksi, joka vaatii suurta henkistä tai fyysistä vaivaa, jotta se voisi tulla tehdyksi menestyksekkäästi, ja täten haaste testaa ihmisen kykyä. Haaste on siis jotakin, joka tiedetään etukäteen sellaiseksi, että se on tehtävä tai käytävä lävitse, jotta päästään haluttuun lopputulokseen ja siihen pääsyyn joudutaan näkemään vaivaa. Suomen kielessä sanalla haaste on myös toinen, oikeidenkäyntiin liittyvä käsite. Tätä merkitystä ei kuitenkaan käytetä tässä tutkimuksessa haaste-sanan yhteydessä.

1.1.3 Finanssiala

Finanssiala koostuu yrityksistä, jotka tarjoavat asiakkailleen pankki-, rahoitus- tai vakuutuspalveluita. Finanssialalla on suuri merkitys niin yksittäisten kotitalouksien ja yritysten, kuin koko yhteiskunnan ja kansantalouden kannalta. Finanssiala mahdollistaa pääomien hankkimisen, lainaamisen, pankkitalletukset, maksuliikenteet, sijoitukset ja vakuutukset, niin yksityisille kotitalouksille kuin myös yrityksille ja instituutioille. Finanssialan tärkeyden takia, ala on tarkasti

säännelty ja valvottu. Suomessa finanssialan valvonnan hoitaa Finanssivalvonta, jonka tavoitteet ja tehtävät on kirjattu lakiin (Finanssivalvonta, 2020a).

1.1.4 FinTech

Finanssiteknologia eli FinTech (Financial Technology) on teknologiaa, jonka avulla tuotetaan pankki-, vakuutus-, rahoitus-, sijoitus- tai maksupalveluita (Finanssivalvonta, 2020b). FinTech yrityksillä tarkoitetaan yrityksiä, jotka tarjoavat tai kehittävät edellä mainittuja palveluita finanssialan yrityksille. FinTech-innovaatioita ovat esimerkiksi kryptovaluutat, chattibotit ja älysopimukset.

1.1.5 Algoritmi

Algoritmi on tarkka yksityiskohtaisesti kuvattu ohje siitä, kuinka tehtävä tai prosessi tulee vaihe vaiheelta suorittaa, jotta prosessi johtaa haluttuun lopputulokseen (Brookshear, 1989). Algoritmi voidaan nähdä eräänlaisena apukeinona tai työkaluna tarkasti kuvaillun ongelman ratkaisemiseksi. Cormen ym. (2009) kertovat algoritmin olevan epävirallisesti mikä tahansa hyvin määritelty laskennallinen menettely, joka ottaa arvon tai arvojoukon syötteenä, ja tuottaa siitä jonkin arvon lopputulosteena. Yksinkertainen esimerkki algoritmista on ruokaresepti, joka kuvaa vaihe vaiheelta yksityiskohtaisesti sen mitä tulee missäkin vaiheessa tehdä, jotta lopputuloksena saadaan haluttu valmis ruoka-annos.

1.2 Tutkimusongelma ja tutkimuskysymykset

Tekoäly on läsnä useilla aloilla jo tänä päivänä ja lähivuosina tekoälyä hyödyntävien yritysten määrä tulee lisääntymään valtavasti. Tutkimuslaitos Gartnerin johtavan analyytikon Christopher Iervolinon mukaan yli neljänneksellä yrityksistä on aikomus ottaa jollakin tasolla tekoälyä hyödyntävät teknologiat käyttöön rahoitusosastoissaan vuoden 2020 aikana (Gartner, 2018). Tekoälyn yleistyessä ja koneiden korvatessa ihmisten tekemää työtä, syntyy myös uudenlaisia haasteita ja riskejä, niin finanssialan yrityksille kuin myös niiden asiakkaille. Pankit ja vakuutusyhtiöt keräävät jo tänä päivänä erittäin paljon erilaista dataa asiakkaistaan. Kerättyä dataa pyritään hyödyntämään liiketoiminnassa tekoälyn avulla, mutta niin koneiden kuin ihmistenkin kohdalla suuret datamäärät voivat tuottaa yritykselle haasteita ja riskejä, kuten esimerkiksi väärintulkitseminen tai vääriin käsiin joutumisen. Tekoälyllä on paljon potentiaalia muuttaa useiden alojen toimintatapoja kokonaan uusiksi ja näin suurissa muutoksissa on aina omat haasteensa. Tekoälyn hyödyistä ja sen hyödyntämisestä löytyy aiempaa tutkimustietoa, lisäksi tekoälystä finanssialalla on myös kertynyt jo jonkin verran aiempaa tutkimusta. Tekoälyn mahdollisia riskejä ja haasteita on myös tutkittu yleisellä tasolla, mutta finanssialan yhteydessä aiempi tutkimus on vielä todella vähäistä.

Finanssialalla tekoälyn yleistymisen mukanaan tuomia uhkia ja haasteita on syytä tutkia kahdesta syystä: Finanssialalla on merkittävä rooli yhteiskunnan sujuvan toimimisen kannalta ja finanssialalla tekoälyä käytetään jo tänä päivänä runsaasti. Tämän tutkimuksen empiirisessä osiossa näitä haasteita ja riskejä tutkitaan nimenomaan Suomen finanssialan yhteydessä. Kirjallisuuskatsaus osiossa tutkitaan, millaista aiempaa tutkimusta aiheesta löytyy maailmalta. Lopuksi pohditaan miten Suomen finanssialan tekoälyn yleistymiseen liittyvät haasteet ja riskit, kohtaavat kansainvälisesti tunnistetut riskit ja haasteet. Tutkimuskysymyksiä muodostui kolme, joista ensimmäiseen vastataan kirjallisuuskatsauksen pohjalta. Toiseen kysymykseen vastataan empiirisen tutkimuksen pohjalta ja kolmas kysymys on tyyliltään apukysymys, kahden ensimmäisen kysymyksen vastausten pohtimisille. Tutkimuskysymykset ovat:

1. Millaisia tekoälyn yleistymiseen liittyviä haasteita tai riskejä finanssialan yritykset kokevat kansainvälisesti?
2. Millaisia tekoälyyn liittyviä haasteita tai riskejä Suomen finanssialalla koetaan ja varaudutaanko niihin?
3. Millaisia eroja tai samankaltaisuuksia finanssialalla koetaan Suomessa ja kansainvälisesti, tekoälyn yleistymisen haasteisiin ja riskeihin liittyen?

1.3 Tutkimuksen rakenne

Tämä pro gradu tutkimus on sisällöltään jaettu seitsemään lukuun alalukuineen. Tutkimus alkaa johdannolla, jossa esitellään tutkimuksen aihe, käydään läpi syitä tutkimuksen tekemiselle, avataan keskeisimmät käsitteet ja kerrotaan mitä, miksi ja kuinka tutkitaan, sekä esitellään tutkimuskysymykset. Tutkimuksen toisessa luvussa keskitytään tekoälyyn terminä. Luvussa esitellään mitä tekoälyllä tarkoitetaan tämän tutkimuksen yhteydessä. Lisäksi käydään lävitse erilaisia tekoälyn osa-alueita ja tasoja. Tutkimuksen kirjallisuuskatsausosio jakautuu kahteen osaan, lukuihin kaksi ja kolme. Luvussa kaksi käydään lävitse tekoälyn lisäksi, Suomen finanssiala, sekä aiempien tutkimusten avulla selvitetään, millaista tekoälyä maailmalla käytetään finanssialan yhteydessä. Luku kolme sisältää kirjallisuuskatsauksen pohjalta koottuja tekoälyyn liittyviä haasteita ja riskejä kansainvälisesti, eri puolilta maailmaa. Luvussa käsitellään myös yleisesti riskiä liiketoiminnan yhteydessä.

Neljännessä luvussa esitellään tämän tutkimuksen empiirinen osuus. Luvussa kerrotaan, miksi kyseinen tutkimusmetodi on valittu tämän tutkimuksen yhteydessä käytettäväksi. Lisäksi siinä käydään lävitse sitä, kuinka empiirinen tutkimus on toteutettu. Viides luku sisältää empiirisen tutkimuksen tulokset. Tämä luku on jaettu kolmeen alalukuun, joista ensimmäinen käsittelee tekoälyn roolia haastateltavien yrityksissä. Toinen alaluku käsittelee käytöstä poistunutta tekoälyä, tulevaisuuden tekoälyä ja tekoälyn hyötyjä haastateltavien yrityk-

sissä. Kolmas alaluku sisältää empiirisen tutkimuksen ydinsisällön, eli tekoälyyn liittyvät haasteet ja riskit Suomen finanssialalla. Luku kuusi pitää sisällään empiirisen tutkimuksen pohjalta tehdyt johtopäätökset, sekä pohdinnan tutkimuksesta. Luvussa käydään myös lävitse mietteitä tämän tutkimuksen luotettavuudesta ja laadukkuudesta. Lisäksi luvun lopussa on ajatuksia mahdollisista jatkotutkimusaiheista, jotka ovat syntyneet tämän tutkimuksen tekemisen aikana. Viimeinen, eli seitsemäs luku pitää sisällään tiiviin yhteenvedon koko pro gradu tutkimuksesta. Tutkimuksen lopussa on lisäksi saatavilla tässä tutkimuksessa käytettyjen viitteiden lähteet, sekä empiirisen tutkimuksen puolistrukturoitu haastattelukysymysten pohja.

2 TEKOÄLY JA SEN SOVELTAMINEN FINANSSIALALLA

Tekoälyllä on useita erilaisia määritelmiä, jotka saattavat hieman poiketa toisistaan, riippuen missä yhteydessä ne on kuvattu. Yhteistä kaikille määritelmille on kuitenkin se, että niissä kone kykenee tekemään asioita, jotka mielletään jollakin tavoin älykkäiksi. Tässä luvussa käsitellään tekoälyn määritelmä tämän tutkimuksen osalta, tekoälyn erilaisia osa-alueita, sekä tekoälyn tasoja. Tämän luvun jälkimmäinen alaluku käsittelee Suomen finanssialaa, sen rakennetta ja sääntelyä. Lisäksi alaluvussa käydään lävitse kirjallisuuskatsauksen pohjalta finanssialalla sovellettavaa tekoälyä.

2.1 Tekoäly

Tekoälyllä on hieman erilaisia määritelmiä, riippuen kontekstista ja käyttötarkoituksesta. Terminä tekoälyä käytetään melko laajasti, aina sudokuja ratkovasta mobiilisovelluksesta itseohjautuviin autoihin. Termin käyttöön liittyy kuitenkin aina jonkinlainen käsitys jostakin koneen suorittamasta älyllisestä toiminnasta. Tässä alaluvussa käydään tarkemmin lävitse, mitä tekoälyllä tarkoitetaan tämän tutkimuksen yhteydessä. Alaluku sisältää lisäksi lyhyen läpikäynnin tekoälyn erilaisista osa-alueista ja tasoista.

2.1.1 Tekoälyn määritelmä

Tekoäly omaa käsitteenä usean kymmenen vuoden historian, sillä ensimmäisten tekoälyä käsittelevien tieteellisten artikkeleiden voidaan katsoa olleen Turingin vuonna 1950 julkaisema ”Computing Machinery and Intelligence” ja Shannonin samana vuonna kirjoittamat tekstit siitä kuinka kone voitaisiin ohjelmoida pelaamaan shakkia (McCarthy & Hayes, 1969). Vuoden 1950 artikkelissaan Alan Turing käsittelee ja ratkoo kysymystä ”voivatko koneet ajatella?” tekemänsä testin perusteella. Testin ideana on, että tarkkailijana toimiva ihmi-

nen ei pysty tekstimuodossa annettujen vastausten pohjalta erottamaan ihmisen ja koneen vastauksia toisistaan, eli siinä kone pyrkii antamaan vastaukset mahdollisimman ihmismäisesti (Turing, 1950). Myöhemmin kyseisestä testistä on ruvettu käyttämään nimeä Turingin testi ja se on noussut tekoälytutkimuksen klassikon maineeseen. Varsinaisena tekoälyn isänä voidaan kuitenkin pitää yhdysvaltalaista John McCarthyä, sillä hän oli ensimmäinen, joka esitteli tekoälytermin (Artificial Intelligence) vuonna 1956 (Siukonen & Neittaanmäki, 2019).

Tekoälyn määritelmä ei kuitenkaan ole aina aivan selkeä ja määritelmä voi hieman vaihdella kontekstin mukaisesti. Tekoälyllä saatetaan tarkoittaa viihdeelokuvassa tai mediassa toisinaan eri asioita kuin mainostoimiston, tietotekniikkayrityksen tai tieteellisen artikkelin yhteydessä. Kaikissa näissä on kuitenkin yhteistä se, että jokaisessa yhteydessä tekoälyn katsotaan liittyvän jollakin tavalla ihmismäiseen älykkyyteen. Mitä sitten on älykkyys? Määritelmiä on useita, joista eräs on, että älykkyys on kyky ratkoa ongelmia tai luoda jotakin jolla on arvoa yhdessä tai useammassa kulttuurillisessa yhteydessä (Gardner, 1999). Ihmisen kohdalla älykkyys lähtee kasvuun nopeasti syntymän jälkeen. Vastasyntyneen ihmislapsen älykkyys on vielä vaatimatonta, mutta se alkaa nousta nopeaan tahtiin. Älykkyyden kehitykseen vaikuttavat perheen, ympäristön ja koulutuksen lisäksi monet muut ulkoiset vaikuttimet. Pienellekään lapselle ei ole ongelma erottaa autoa omenasta, ei fyysisesti eikä kuvasta tunnistamalla. Tämänhetkiset tekoälyä hyödyntävät sovellukset eivät kuitenkaan vielä pysty oppimaan fyysisistä kokemuksista yhtä hyvin kuin pieni lapsi, eivätkä ne ymmärrä kieltä tarpeeksi hyvin oppiakseen lukemastaan (McCarthy, 2007).

2.1.2 Tekoälyn osa-alueet ja tasot

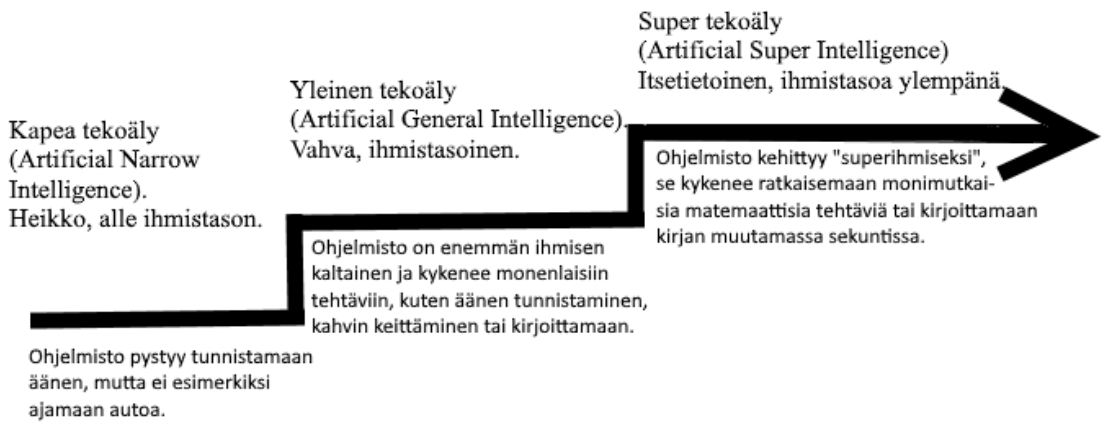
Tekoäly voidaan myös jakaa osa-alueisiin, kuten koneoppimiseen (Machine Learning), syväoppimiseen ja neuroverkkoihin (Deep Learning & Neural Networks) ja robotiikkaan. Koneoppimisessa ohjelmistolle on syötetty algoritmeja, joiden avulla se pääsee haluttuun lopputulokseen. Kaikista mahdollisista tilanteista ei kuitenkaan tehdä valmiita algoritmeja, vaan tarkoituksena on, että ohjelmisto oppii itsenäisesti datan avulla pääsemään lopputulokseen. Esimerkkeinä koneoppia hyödyntävistä ohjelmistoista on muun muassa hakukoneohjelmisto, joka pystyy korjaamaan kirjoitusvirheet tai roskapostisuodatin, joka osaa suodattaa "roskat" tärkeistä sähköposteista.

Neuroverkko on laskentamalli, joka on saanut inspiraation aivojen hermo-, eli neuroverkko rakenteesta (Shalev-Shwartz & Ben-David, 2014). Toisin sanoen ihmisen todellista aivotoimintaa mallinnetaan virtuaalisten neuroneiden avulla kerroksittain. Syväoppimisessa taas yhdistetään raakadatan hyödyntäminen neuroverkkojen toimintamalliin. Neuroverkkoja hyödyntäviä ohjelmistoja ovat esimerkiksi mobiilisovellus, joka pystyy muuttamaan puheen tekstiksi tai persoonalliset suositusehdotukset, joita tarjoavat palveluissaan mm. Netflix, Spotify ja Amazon.

Robotiikka nähdään joissain kirjoituksissa tekoälystä erillisenä omana alueenaan, mutta tässä tutkimuksessa se on parasta esittää tekoälyn osa-alueena.

Eri tasoisia robotteja on ollut olemassa jo yli puoli vuosi sataa (Hockstein ym., 2007). Robotteja käytetään useissa eri yhteyksissä eri tarkoituksiin. Esimerkkeinä voidaan mainita palvelurobotit, teollisuusrobotit, ohjelmistorobotit ja opetusrobotit. Robotiikassa, varsinkin kehittyneiden robottien yhteydessä on yleensä yhteistä se, että niissä yhdistyy useita eri tekoälyn osa-alueita koneoppimisesta kuvan- ja äänentunnistukseen. Tämän lisäksi roboteissa käytetään hyväksi myös kameroita ja sensoreita, jotta robotin työskentelystä saadaan entistä tarkempaa ja luotettavampaa. Robotit pystyvät jo tänä päivänä korvaamaan joitakin aiemmin ihmisen tekemiä töitä. Siitä huolimatta, että robottien kehittäminen ja hankkiminen on vielä yksittäiselle yritykselle kallista, niin ne ovat usein taloudellisesti kannattavia, sillä robotilla ei ole työaikoja, sille ei tarvitse maksaa palkkaa, se ei sairasta, eikä siitä koidu työnantajan sivukulumaksuja (Brougham & Haar, 2018).

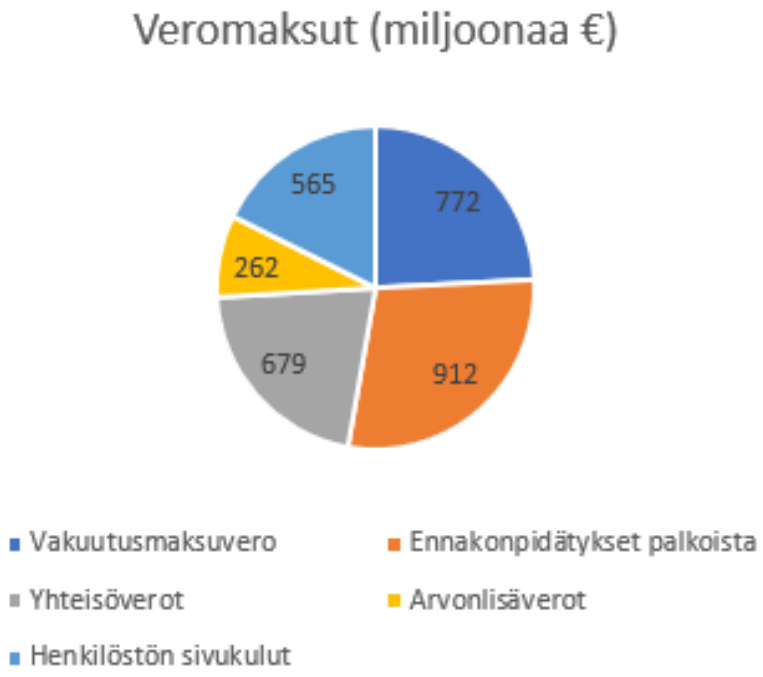
Tekoäly voidaan jaotella myös eri tasoihin, Kaplan ja Haenlein (2019) jakavat tekoälyn kolmeen eri tasoon: kapeaan, heikkoon ja supertekoälyyn (Kuvio 1). Kapea tekoäly edustaa tasoista alinta. Se nähdään älykkyydeltään heikkona, alle ihmistason älykkyyden. Tällä tasolla tekoälyohjelmisto pystyy tunnistamaan esimerkiksi äänen, mutta ei täysin ajamaan itsenäisesti autoa. Keskimmäistä tasoa kutsutaan yleiseksi tekoälyksi, se on älyltään ihmisen tasolla. Tällä tasolla tekoälyohjelmisto kykenee monimutkaisempiin tehtäviin ja se kykenee suorittamaan niitä samaan aikaan, sekä erottelemaan tehtävät toisistaan. Tällä hetkellä kaikki maailmassa oleva tekoäly on kapean tekoälyn tasolla matkalla kohti yleistä tekoälyä. Tekoälyn ylimpänä tasona nähdään niin kutsuttu supertekoäly. Tällä tasolla oleva tekoälyohjelmisto on täysin itsetietoinen ja sen älykkyyden taso on ihmistä korkeammalla. Supertekoäly kykenee suorittamaan ja ratkaisemaan monimutkaisia matemaattisia tehtäviä tai kirjoittamaan täysimittaisen kirjan halutusta aiheesta muutamassa sekunnissa.



KUVIO 1 Tekoälyn tasot (Kaplan & Haenlein, 2019)

2.2 Finanssiala Suomessa

Finanssialalla on Suomessa tärkeä yhteiskunnallinen rooli. Ala mahdollistaa niin yrityksille, yksityisille kotitalouksille kuin institutionaalisille toimijoille lainan saannin, sijoittamisen, vakuuttamisen, pääomien liikkumisen ja talletukset. Finanssiala on myös merkittävä verotulojen tuottaja yhteiskunnalle. Vuonna 2018 ala tuotti verotuloja noin 3,2 miljardia euroa (Lapatto, 2019). Verotulot koostuivat vakuutusmaksuveroista, yhteisöveroista, arvonlisäveroista, henkilöstön sivukuluista ja palkkojen ennakonpidätyksistä (kuvio 2). Lähes jokainen ihminen on syntymästään kuolemaan asti jonkin finanssialan yrityksen asiakas. Yrityksille kertyy tietoa asiakkaiden palkkatuloista, veloista, maksukyvystä, tilitapahtumista ja henkilötiedoista. Henkilökohtaisten ja arkaluontoisten tietojen keräämiseen, taltiointiin ja käyttämiseen liittyy aina riskejä ja tästä syystä yhdessä tärkeän yhteiskunnallisen merkittävyyden kanssa, finanssiala on Suomessa erittäin tarkoin säännelty ja valvottu.



KUVIO 2 Finanssialan veromaksut (Finanssiala, 2019)

2.2.1 Finanssialan rakenne

Finanssiala koostuu yrityksistä, jotka tarjoavat asiakkailleen pankki-, vakuutus- tai rahoituspalveluita. Pankit voidaan jakaa vähittäispankkeihin, investointipankkeihin ja keskuspankkeihin. Suomessa yleisin vähittäispankkimuoto on osakeyhtiömuotoiset liikepankit. Muita vähittäispankkimuotoja Suomessa on osuuspankit, säästöpankit ja hypoteekkipankit, joiden toimiala koostuu pelkästään asuntolainojen myöntämisestä. Näiden lisäksi Suomessa toimii yksityis-

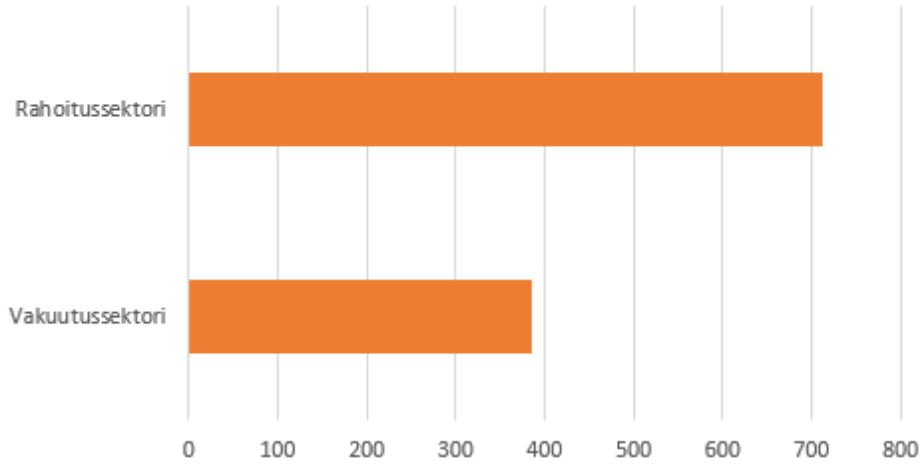
pankkeja, jotka tarjoavat asiakkailleen usein myös neuvontaa laki- ja veroasioissa. Investointipankkien pääasiallinen tehtävä on auttaa instituutioita, valtioita ja yrityksiä keräämään pääomia. Tämä tapahtuu laskemalla liikkeelle arvopapereita sekä johdannaisia, joilla voidaan myöhemmin käydä kauppaa pörsseissä. Investointipankit tarjoavat myös neuvontaa yrityskauppoihin ja yritysten yhdistymisiin liittyen. Vakuutusyhtiöt voidaan jakaa henki-, vahinko- ja työeläkevakuusyhtiöihin. Rahoitusyhtiöt tarjoavat rahoitusta yksityisille kotitalouksille ja yrityksille useisiin erilaisiin tavaroihin tai palveluihin takaisin maksettavaa korkoa vastaan.

Aiemmin mainittujen tahojen lisäksi finanssialaan liittyy myös keskuspankki tai Suomen tapauksessa keskuspankit; Suomen Pankki ja Euroopan keskuspankki. Ensisijaisena tavoitteena Euroopan keskuspankilla on ylläpitää hintatason vakautta korkotasoa ja valuuttamääriä säätelemällä, lisäksi Euroopan keskuspankilla on yksinoikeus setelien liikkeeseenlaskuun euroalueella (Euroopan keskuspankki, 2020). Vuonna 1999 käyttöönotettu Euro ei olennaisesti muuttanut Suomen Pankille perinteisesti kuuluneita tehtäviä. Suurimpana erona on, että nykyisin Suomen Pankki ei toimi pelkästään kansalliselta pohjalta vaan osana keskuspankkien eurojärjestelmää (Suomen Pankki, 2020a). Suomen Pankin tehtäviin kuuluu rahapolitiikan valmistelu ja toteutus Suomessa, rahoitusjärjestelmän valvominen, tilastojen tuottaminen, pankkien välisten maksujen selvityksistä huolehtiminen sekä tehokkaiden maksujärjestelmien ylläpitäminen (Suomen Pankki, 2020b).

2.2.2 Finanssialan sääntely

Usean muiden valtioiden tapaan, myös Suomessa finanssiala on erittäin tarkasti säännelty. Suomessa sääntelystä vastaa Finanssivalvonta ja sille asetetut tavoitteet ja tehtävät on kirjattu lakiin (Finlex, 2008). Näihin tavoitteisiin kuuluu muun muassa finanssimarkkinoiden vakauden edellyttämä valvottavien vakaa toiminta, vakuutettujen etujen turvaaminen, yleisen luottamuksen säilyminen, hyvien menettelytapojen noudattamisen edistäminen finanssimarkkinoilla sekä lisätä yleisön tietämystä finanssimarkkinoista (Finanssivalvonta, 2020c). Finanssivalvonnan toiminta on pääasiassa rahoitettu valvottavilta perityiltä valvontamaksuilla, lisäksi pienempi osuus rahoituksesta tulee Suomen Pankilta (Finanssivalvonta, 2018a).

Valvottavat koostuvat usean toimialan yrityksistä, kuten pankeista, työttömyyskassoista, vakuutusyhtiöistä ja pörssistä. Vuoden 2019 lopussa valvottavien kokonaismäärä oli 1098 yritystä (Finanssivalvonta, 2020d), joista 713 kuului rahoitussektorin valvottaviin ja 385 yritystä vakuutussektoriin (kuvio 3).



KUVIO 3. Valvottavien jakauma (Finanssivalvonta, 2020d)

Finanssialaa koskee kansalliset lait, EU-lainsäädännöt ja suositukset. Tämän lisäksi finanssialalla toimivilta yrityksiltä oletetaan myös oma-aloitteista varautumista niin normaaliolojen häiriötilanteisiin, kuin myös poikkeusoloissa, sillä rahoitusmarkkinapalveluiden keskeyttämätön tarjonta on välttämätöntä koko kansantalouden toiminnalle (Finanssivalvonta, 2020e). Säännöksiä ja lakeja valvova finanssivalvonta voi langettaa valvottaville sanktiota väärinkäytöksistä ja rikkomuksista. Sanktiot voivat olla julkisia varoituksia, rikemaksuja tai seuraamusmaksuja (Finanssivalvonta, 2018b).

2.3 Tekoäly finanssialalla

Terveydenhuollon ohella finanssialaa voidaan pitää yhtenä tekoälyn käytön ensimmäisinä omaksujina. Finanssialalla tekoälyä on käytössä jo tänä päivänä usealla eri osa-alueella. Tässä alaluvussa käydään lävitse kirjallisuuskatsauksen pohjalta, millaisissa asioissa tekoälyä finanssialalla käytetään. Käyttötavat ovat jaoteltu tässä osiossa eri tekoälymetodien mukaisesti.

2.3.1 Koneoppimisen metodit

Koneoppimisen teknologioita hyödyntäviä tekoälysovelluksia on käytössä finanssialalla useisiin eri tarkoituksiin. Eräs yleisimmistä käyttötarkoituksista on asiakaskohtaisten luottoriskien arviointi tekoälyn avulla. Pankki myöntää asiakkaalle tietyn suuruisen luottorajan ja myöntämisen jälkeen asiakkaan luottokelpoisuutta seurataan myös aktiivisesti. Luoton määrää voidaan nostaa tai asiakkaalta perittävää korkoa voidaan laskea tai tapauskohtaisesti nostaa, riippuen asiakkaan maksukäyttämisestä (Khandani ym., 2010). Tunnistaakseen kor-

keanriskin asiakkaat pankkien täytyy vertailla ja tutkia asiakkaistaan saatavilla olevia tietoja ja tehdä päätökset näiden aiempien tapahtumien pohjalta. Koneoppimisen algoritmit pystyvät tekemään vertailut ja tuottamaan tulokset ihmistä tehokkaammin ja tarkemmin, kuitenkin käyttäen ihmismäisiä päätöksenteon menetelmiä. Khandani, Kim ja Lo (2010) toteuttivat tutkimuksen, jossa he käyttivät Yhdysvaltalaispankkien asiakkaistaan vuosina 2005-2009 keräämää dataa. Tämän pohjalta he kehittivät koneoppimisen keinoja käyttävän mallin, jonka lopputulos pystyi tekemään 6–23 % säästöt luottoriskeistä syntyviin tappioihin. Säästetyt prosentit vaihtelivat pankkien välillä, mutta otettaessa huomioon Yhdysvaltalaispankkien suuret liikevaihdot ja tuotot, niin jo skaalan alareunan 6 prosentin parannukset tarkoittavat useiden miljoonien säästöjä.

Toinen alue, jossa koneoppimisen teknologioita käytetään paljon finanssialalla, on vakuuttamisen yhteydessä vakuutuspetokset ja niiden tunnistaminen. Vakuutusyhtiöillä on motiivi kehittää tekoälyä tunnistamaan asiakkaiden petosyritykset, sillä vakuutusyhtiöiden korvaussummista 10–30 % koostuu vakuutuspetoksista ja joissakin erityisvakuutusten tapauksissa luku nousee jopa 50 prosenttiin (Tao ym., 2012). Vakuutuspetoksia voi olla ihmisen vaikea tunnistaa ja tutkimukset osoittavat todennäköisyyden sille, että vakuutusyhtiön henkilökunta tunnistaa petoksen, olevan noin 1/3 (Caron & Dionne, 1999). Autovakuutusten kohdalla on näyttöä, että kone vastaavasti tunnistaa petoksista yli 70 % (Artis ym., 2002). Vakuutuspetosten tutkiminen perinteisin keinoin on paljon aikaa vievää toimintaa ja se vaatii runsaasti työtunteja työntekijöiltä. Tekoäly pystyy samasta asiasta suoriutumaan huomattavasti ihmistä nopeammin, luoden säästöjä samalla kun työntekijät voivat keskittyä muihin toimintoihin. Vakuutusyhtiöiden tappiot ovat valtavia petosten takia, esimerkiksi Yhdysvalloissa vuonna 2003, pelkästään sairasvakuutuksien väärinkäytökset ovat aiheuttaneet vakuutusyhtiöille yli 51 miljardin dollarin tappiot (Peng ym., 2006).

Koneoppimista hyödynnetään myös sijoitussalkkujen riskitasojen ja tuottojen arvioimiseen. Maailman suurin varainhoitoyhtiö BlackRock tarjoaa niin yksityisille sijoittajille kuin heidän omille varainhoitajille käyttöönsä Aladdin nimisen alustan. Aladdin pystyy automaattisesti seuraamaan korkoja, valuuttakursseja sekä yli 2000 muuta riskeihin liittyvää tekijää päivässä, lisäksi se kykenee testaamaan sijoitussalkun kehitystä erilaisissa taloudellisissa olosuhteissa (BlackRock, 2020).

2.3.2 Datan louhinnan metodit

Pankit, vakuutusyhtiöt ja rahoituslaitokset hyödyntävät tekoälyä myös tehdessään asiakasanalyysejä. Mansingh (2015) tutki jamaikalaisia internetpankin käyttäjiä KDDM-menetelmällä (Knowledge Discovery and Data Mining), jonka etuihin kuuluu se, että menetelmä sisältää yhden mallin sijasta useammasta mallista koostuvan mallisarjan. Hänen tutkimuksessaan otettiin huomioon asenteellisten ja käyttäytymisperusteisten muuttujien lisäksi demograafiset, eli väestön määrää ja rakennetta, sekä maantieteellistä jakautumista kuvaavat muuttujat. Mitä enemmän huomioonotettavia seikkoja malliin otetaan, niin re-

levantimpaa dataa tiedonlouhinta yrityksille asiakkaistaan tarjoaa.

Datan louhinnan metodeja hyödyntäviä tekoälysovelluksia käytetään myös finanssialan yritysten valvontaan. Yritysten laatimista finanssiraporteista on mahdollista louhia petoksiin viittaavia yksityiskohtia (Glancy & Yadav, 2011). Samaa tekniikkaa voisi teoriassa käyttää myös yritysten arvonmäärittämiseen tai ainakin sen tukena.

2.3.3 Syväoppimisen metodit

Syväoppiminen on tekoälyn alue, jossa hyödynnetään neuroverkkoja useassa kerroksessa (Patterson & Gibson, 2017). Syväoppimisen metodeja käytetään sellaisissa asioissa missä ihminen on yleensä melko hyvä, kun käsiteltävä datamäärä on pieni. Esimerkkinä voidaan mainita asioiden ennustaminen pienillä tiedoilla, mutta kun tiedon määrä kasvaa niin kone kykenee toimimaan monin verroin ihmistä tarkemmin ja tehokkaammin. Tästä syystä syväoppimista ja neuroverkkoja hyödyntäviä tekoäly sovelluksia on käytössä ympäri maailman useissa finanssialan yrityksissä. Toisin kuin monet muut tekoälyn osa-alueet, neuroverkot jäljittelevät jossain määrin ihmisen aivojen prosessointiominaisuuksia ja tämän seurauksena hermoverkot voivat tehdä johtopäätöksiä epätäydellisistä tiedoista, tunnistaa kuviot reaaliajassa ja ennustaa tulevaisuutta (Trippi & Turban, 1992).

Syväoppimisen monipuoliset mahdollisuudet ovat johtaneet siihen, että sitä hyödyntäviä sovelluksia käytetään esimerkiksi seuraavien asioiden tehostamiseen; osakekurssien ennustamiseen, arvopaperikauppajärjestelmien kehittämiseen, joukkolainojen luokituksen ennustamiseen, valuuttamarkkinoiden mallintamiseen ja taloudellisten vaikeuksien ennustamiseen, kulutus- ja asuntolainojen sekä luottokorttien maksukyvyttömyysriskin arviointiin (Swamy ym., 1997). Mastercard luottokorttiyhtiöllä on käytössä Threat Scan sovellus, joka auttaa pankkeja ympäri maailman ennakoimaan mahdollisiin haavoittuvaisuuksiin, jäljittelemällä ennakoivasti tunnettua rikollista toimintaa, jotta voidaan arvioida järjestelmän vastustuskykyä ennen hyväksikäytön ja petoksen tapahtumista (Saidam, 2019). Tekoälyn hyödyntäminen rikollisen toiminnan torjuntaan on erityisen tärkeätä juuri finanssialalla, sillä Boston Consulting Groupin raportin (2019) mukaan kyberhyökkäykset kohdistuvat finanssialan yrityksiin 300 kertaa muita aloja useammin.

2.3.4 Kuvan- ja kasvojentunnistamisen metodit

Finanssialan yhteydessä kuvan- ja kasvojentunnistamista hyödyntävät tekoälyohjelmistot eivät vielä toistaiseksi ainakaan ole kovin yleisiä. Joitakin esimerkkejä käytöstä kuitenkin on. Esimerkkinä kuvantunnistusohjelmistot, jotka auttavat paperiasiakirjojen digitoinnissa. Pankkien ja vakuutusyhtiöiden työntekijät voisivat skannata paperiasiakirjat PDF-tiedostoiksi ja ladata ne asiakirjojen digitointiohjelmistoon, jonka jälkeen konenäköalgoritmi voi käydä PDF-

tiedostot läpi ja lukea asiakirjan sanoja täyttämällä asiakirjan digitaalisen version kentät PDF-tiedostossa olevilla sanoilla (Azulay, 2019).

Kiinassa valtio on luonut tekoälyn ja satojen miljoonien valvontakameroiden avulla kansalaisia valvovan digitaalisen infrastruktuurin. Kasvojen tunnistusteknologiaa hyödynnetään esimerkiksi pankkiautomaattien yhteydessä. Kasvojentunnistusta käytetään myös kansalaisten sosiaaliseen pisteytykseen ja hyvä pisteitys helpottaa esimerkiksi pankkilainan saamista tai lainan saamista alhaisemmalla korolla (Kostka, 2019).

2.3.5 Puheentunnistus, luonnollisen kielen prosessit ja robotiikka

Robotiikka tai ohjelmistorobotiikka (engl. Robotic Process Automation, RPA) on uudenlainen ohjelmistojen käyttötapa liiketoimintaprosessien automatisoimiseksi murto-osalla perinteisten ratkaisujen kustannuksista ilman, että tarvitsee muuttaa nykyisiä IT-järjestelmiä (Lamberton ym., 2017). Finanssialan yritykset ympäri maailman ovat omaksuneet robotiikkaa hyödyntävät tekoälysovellukset ja niitä käytetäänkin jo usean toiminnon yhteydessä. Esimerkiksi yksi Yhdysvaltojen suurimmista rahoitusyhtiöistä JP Morgan Chase on jo jonkin aikaa hyödyntänyt menestyksekkäästi robotiikkaa suorittamaan tehtäviä, kuten tietojen keräämistä, asiakirjojen tallentamista, maksuneuvonta-sähköpostiviestien tietojen tunnistamiseen ja todentamiseen, sekä asiakkaan tuntemiseen velvoittavien säännösten ja määräysten noudattamiseen (J.P Morgan, 2020).

Monelle finanssialan yrityksen asiakkaalle asiakaspalvelun yhteydessä tulleet ns. chattibotit ovat myös robotiikkaa hyödyntäviä tekoälysovelluksia. Ne pystyvät vastaamaan yksinkertaisempiin asiakkaan kysymyksiin itsenäisesti tai ohjaamaan asiakkaan eteenpäin oikeaan paikkaan. Hieman kehittyneemmät chattibotit tunnistavat asiakkaan kirjoittamia sanoja ja lauseita ja pystyvät hakemaan niiden perusteella tietoja yrityksen sisäisistä tietokannoista. Yhä useammassa yrityksessä chattibotti on ensimmäinen kohtaaminen, mikä asiakkaalle tulee vastaan asiakaspalvelua etsittäessä. Toisinaan chattibotin kanssa asioiminen voi olla myös turhauttavaa, mutta siitä huolimatta se tehostaa yrityksen toimintaa, sillä varsinainen ihmis-asiakaspalvelija näkee suoraan mitä asiakas on jo kirjoittanut chattibotin kanssa ja täten hän pystyy rajaamaan nopeammin asiakkaan asian oikeaan alueeseen.

Kanadalaispankki Royal Bank of Canada on menestyksekkäästi saanut jo yli miljoona asiakastaan käyttämään pankin tarjoamaa robotiikkaa hyödyntävää MyAdvisor-palvelua (RBC, 2019). Kyseisessä palvelussa asiakkaat voivat saada interaktiivista taloudellista neuvontaa ja reaaliaikaista sijoitusneuvontaa. Lisäksi pankki tarjoaa asiakkailleen NOMI-mobiilisovelluksen. Tekoälyä hyödyntävän NOMI:n avulla asiakkaat voivat hallita päivittäistä talouttaan paremmin, löytää mahdollisia säästökohteita arjestaan ja tunnistaa sijoittamisen trendejä (RBC, 2019).

3 TEKOÄLYN HAASTEET JA RISKIT FINANSSIALALLA

Kaikki haasteet ja riskit eivät ole ainoastaan finanssialaa koskevia, vaan niitä kohdataan myös muilla aloilla, joissa tekoälyä käytetään. Tekoälyn tekniikat, ohjelmistot ja ratkaisut ovat samankaltaisia, omaavat samoja piirteitä riskeihin nähden tai ovat jopa täysin samanlaisia alasta riippumatta. Esimerkiksi terveydenhuollossa tapahtuva tekoälystä johtuva asiakkaiden tietovuoto olisi myös finanssialalla tapahtuen vakava asia, joka johtaisi jälkitoimenpiteisiin. Tämän luvun ensimmäinen alaluku käsittelee riskiä yleisemmällä tasolla, minkä tahansa liiketoiminnan yhteydessä. Toinen alaluku keskittyy tekoälyyn liittyviin haasteisiin sekä riskeihin ja kolmannessa alaluvussa pohditaan kirjallisuuskatsauksesta saatuja tuloksia.

3.1 Riski liiketoiminnan yhteydessä

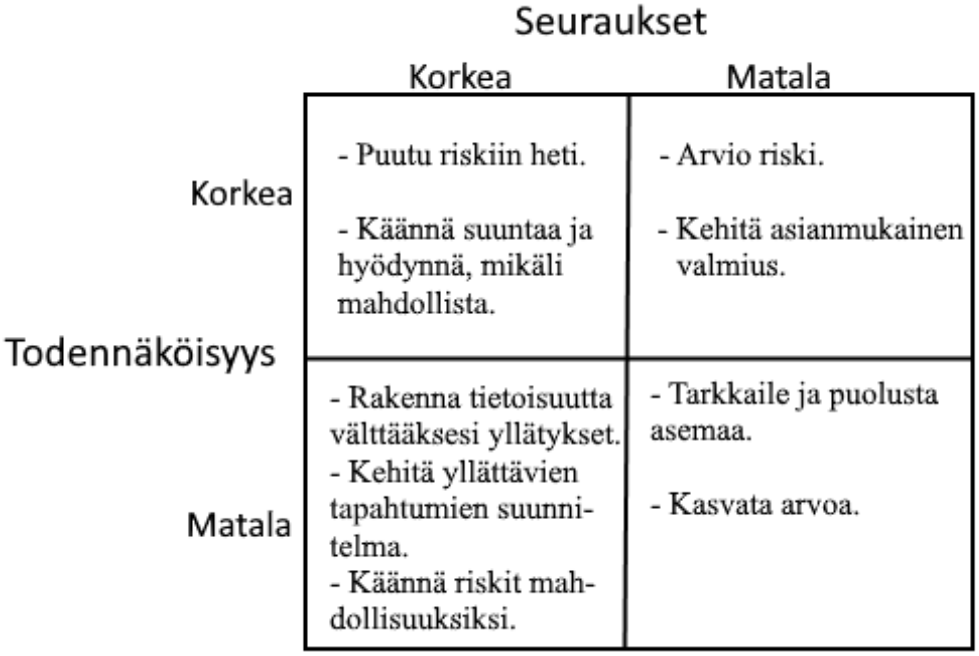
Riskien mittaaminen ja hallitseminen on yksi suurimmista huolenaiheista kaikessa nykyaikaisessa ihmisen toiminnassa, eikä finanssiala ole poikkeus (Bouchaud & Potters, 2000). Riskin määritelmä riippuu kuitenkin hieman kontekstista, sillä ihmisten arkipuheessa riskillä tarkoitetaan mitä tahansa onnettomuuden mahdollisuuteen liittyvää vaaraa tai epätietoisuutta (Kuusela & Ollikainen, 2005). Liiketoimintaa harjoitettaessa yrityksillä on kuitenkin tarve määritellä ja tunnistaa riskit arkipuhetta tarkemmin, jotta riskeihin pystytään varautumaan ja niiden vaikutuksia minimoimaan. Riskien tunnistamisen helpottamiseksi on luotu erilaisia riskien lajitteluita. Jaottelu voi tapahtua esimerkiksi sen mukaan, mihin yrityksen toimintoon mahdollinen riski voisi vaikuttaa. Drew (2007) jakaa yritysten todennäköisesti kohtaamat riskit neljään luokkaan: taloudellisiin, strategisiin ja toiminnallisiin riskeihin, sekä ulkoisiin vaaroihin. Riskien jakaminen eri luokkiin, auttaa riskien todennäköisyyksien ja seuraamuksien arvioinnissa. Riskeihin varautuakseen, yritysten tulisi laatia riskistrategia. Drewn (2007) mukaan riskistrategia määrittelee riskistä selviytymisen pääpiirteet ja määrittelee lähestymistavan, jota tulisi noudattaa koko organisaa-

tiossa. Lisäksi hän listaa seuraavanlaisia asioita, joista mahdollisimman usean tulisi löytyä yrityksen riskistrategiasta:

- Riskiin kohdistuvat vastuut organisaatiossa
- Yrityksen suhtautuminen riskeihin
- Sellaisten tilanteiden hallinta, joissa valvonnan epäonnistuminen johtaa riskien merkittävään toteutumiseen
- Menetelmä, jonka mukaan riskikysymykset on otettava huomioon liiketoiminnan suunnittelun jokaisella tasolla
- Korostetaan riskiä mahdollisuutena ja uhkana
- Vertaisarvioinnin ja riskien vertailuanalyysin edistäminen tarvittaessa
- Kannustetaan ennakoivaan riskien ilmoittamiseen koko yrityksessä
- Sellaisten uusien toimintojen tunnistaminen, joiden riski on arvioitava ja sisällytettävä riskienhallintatoimintoihin
- Riskien hallinnan seurannan, tarkastelun ja varmuuden saamisen tarpeen määritteleminen
- Täsmennetään tarve sellaisille yhteisille perusteille, jotka antavat tietoa riskinarvioinnista ja määritellään erityiset riskit kriittisiksi
- Riskisalkun tasapainottamisen edistäminen ja riskinottohalukkuuden luominen
- Tuetaan tehokasta innovaatiota ja kannustetaan hyvin hallittuun riskinottoon, jotta yrityksen tavoitteet voidaan saavuttaa paremmin
- Riskienhallinnan integrointi vakiintuneisiin menettelyihin ja järjestelyihin
- Kannustamalla tehokasta viestintää riskeistä henkilöstölle ja kaikille sidosryhmille yrityksen sisällä ja ulkopuolella.

Liiketoiminnan riskistrategioissaan yritysten tulisi pohtia myös riskien todennäköisyyksiä, mahdollisia vaikutuksia ja kuinka toimia näiden vaikutusten ja

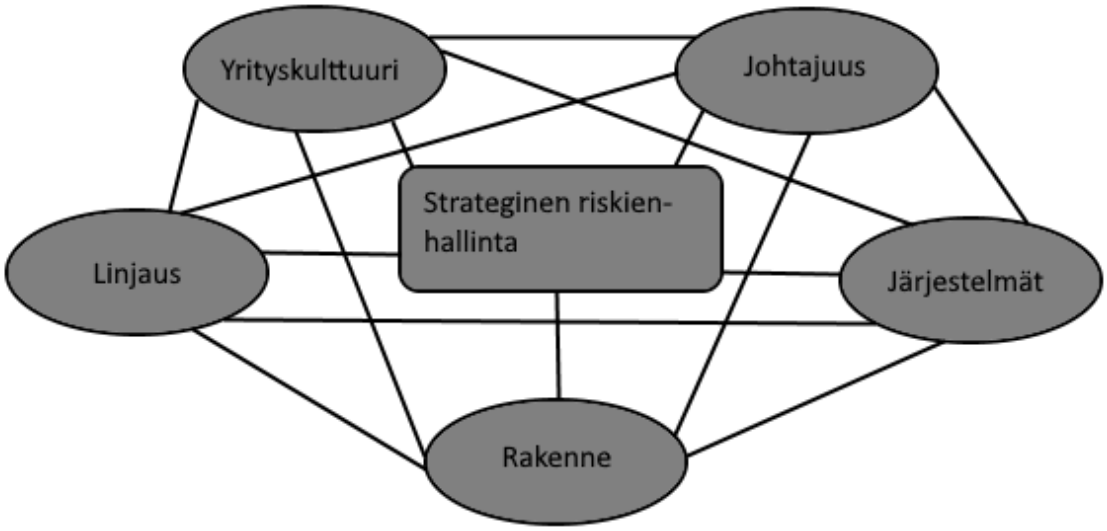
todennäköisyyksien muodostamissa erilaisissa tilanteissa. Drew ja Kendrick (2005) ovat muodostaneet selkeän kuvan avustamaan päätöksentekoa erilaisissa skenaarioissa (kuvio 4). Heidän mallissaan tapahtumaan, jolla on suuri todennäköisyys ja korkeat, eli vakavat seuraukset, tulisi kyseiseen riskiin puuttua heti ja kääntää riskin suuntaa, sekä pyrkiä hyötymään riskistä, mikäli se on mahdollista. Tapahtuma, jolla on korkea todennäköisyys, mutta seuraukset ovat matalaa tasoa, niin tällaisen tapauksen riskiä tulisi arvioida uudelleen, sekä kehittää asianmukainen valmius tapahtuman konkretisoitumiselle. Matalan todennäköisyyden ja vakavien seurausten tapahtumassa tulisi rakentaa tietoisuutta, jotta vältytään suurilta yllätyksiltä. Lisäksi tulisi kehittää suunnitelma yllättävien tapahtumien varalle, sekä tilanteen salliessa, yrittää kääntää riskit mahdollisuuksiksi. Mikäli sekä todennäköisyys, että seuraukset ovat matalalla tasolla niin tulisi tarkkailla ja puolustaa asemaa. Toisin sanoen tämä tarkoittaa, sitä, että ollaan reaktio valmiina, mikäli tilanne muuttuu ja pyritään pitämään tilanne ennallaan mahdollisuuksien mukaisesti. Yrityksen kannalta tämän kaltainen tapahtuma on suotuisa, jos siinä pystytään kasvattamaan arvoa riskin todennäköisyyden ollessa matala ja mahdollisten seuraustenkin ollessa lieviä.



KUVIO 4 Riskiperusteinen päätöksenteko (Drew & Kendrick, 2005).

Välttääkseen riskiin liittyviä strategisia epäonnistumisia, Drew, Kelley ja Kendrick (2006) tunnistivat viisi toisiinsa yhteydessä olevaa elementtiä, joiden avulla yrityksen riskien hallinnalle voidaan luoda tukeva pohja, yhdessä yrityksen hallinnointi- ja ohjausjärjestelmän kanssa (Corporate governance). Nämä viisi CLASS-termillä kutsuttua elementtiä ovat yrityskulttuuri (Culture), johtajuus (Leadership), linjaus (Alignment), järjestelmät (Systems) ja rakenne (Structure) (kuvio 5). Yrityskulttuurilla voi Drewn ym. (2006) mukaan olla positiivisia tai

negatiivisia vaikutuksia, riippuen yrityksen yleisestä tavasta toimia ja hoitaa asioita. He esittävät esimerkkikysymyksiä, joiden avulla yrityskulttuuria on helpompi pohtia. Tällaisia kysymyksiä oli muun muassa, uskaltavatko työntekijät tuoda vapaasti ilmi ongelmia, ilman pelkoa tai mahdollisia haitallisia seuraamuksia tai kannustavatko yrityksen suunnitelmat työntekijöitä toimimaan epäeettisesti tai laittomasti. Johtajuuden kohdalla he esittivät pohdittavia kysymyksiä, kuten osoittavatko johtajat herkkyyttä sidosryhmiä kohtaan tai motivoiko johtajia yrityksen pitkäaikaiset tavoitteet vai lyhyen aikavälin osakekurssin nousu. Linjauksen kohdalla heidän kysymyksensä koskivat sitä, onko yrityksen viimeaikaiset toimet ja suorituskyky todisteena vääristä prioriteeteista tai onko yrityksen hallituksella ja ylimmällä johdolla yhdenmukaiset käsitykset parhaista riskienhallinnan ja sisäisen viestinnän metodeista. Järjestelmien kohdalla he miettivät muun muassa, onko yrityksellä tehokkaat ja standardoidut järjestelmät sisäiseen valvontaan ja taloudelliseen raportointiin. Rakenteen kohdalla he esittivät kysymyksiä, kuten onko hallituksen puheenjohtajan ja toimitusjohtajan roolit yhdistetty ja aiheuttaako tämä ristiriitoja, sekä tarjoaako yritysrakenne tehokkaan ja tasapainoisen menetelmän strategiselle päätöksenteolle. Nämä viisi elementtiä yhdessä yrityksen hallinto- ja ohjausjärjestelmän kanssa luovat vahvan pohjan strategiselle riskienhallinalle.



KUVIO 5 Riskienhallinnan CLASS-elementit (Drew ym., 2006).

3.2 Tekoälyn haasteet ja riskit

Eräs yleisin tekoälyn käytön yleistymiseen liittyvä haaste, niin tutkimuksissa, kuin monien ihmisten ajatuksissa, on huoli siitä, että tekoäly korvaa kokonaan tai osittain ihmisten työpaikat. Huang ja Rust (2018) kehittivät teorian tekoälyllä työpaikkojen korvaamisesta. Heidän teoriansa määrittelee neljä palvelutehtä-

viin tarvittavaa älykkyyttä tai älykkyyden osa-aluetta: mekaaninen, analyyttinen, intuitiivinen ja empaattinen. Lisäksi teoriassa esitetään tapa, jolla yritysten tulisi päättää valitako ihminen vai kone töiden suorittamiseksi. Yksi Huangin ja Rustin (2018) teorian tärkeä merkitys on, että analyyttiset taidot tulevat entistä vähemmän tärkeiksi tulevaisuudessa, kun tekoäly vie enemmän analyyttisiä tehtäviä, joissa vaaditaan analyyttisiä taitoja. Kone pystyy ihmistä tarkemmin ja tehokkaammin hoitamaan analytiikan, jolloin varsinkin empaattisille taidoille on entistä enemmän kysyntää palvelun suorittavan työntekijän ominaisuuksien joukossa.

Yleisesti ehkä ajatellaan tekoälyn korvaavan lähinnä matalapalkkaisia työtehtäviä tai niin kutsuttuja liukuhihnatöitä, jotka robotti pystyy hoitamaan ihmisen sijasta. On kuitenkin näyttöä, että tekoälyllä on pystytty korvaamaan myös korkeaa koulutusta vaativia tehtäviä, kuten esimerkiksi rahastoportfoliota johtavan henkilön tehtävät (Javelosa, 2017). BlackRock on maailman suurin varainhoitaja ja Javelosan (2017) mukaan heillä on suunnitelmissa yhdistää perinteisen sijoittamisen metodit ja tekoäly, tästä tulee seuraamaan jopa 13 % nykyisten rahastonhoitajien työsuhteen loppuminen. Tämä esimerkki sopii melko hyvin myös aiemmin mainitun Huangin ja Rustin (2018) teoriaan tekoälyä analytiikkaa vaativien tehtävien korvaajana.

Nykyisten tekoälyratkaisuiden kehittyminen tuo mukanaan myös entistä suuremmat tietoturvahaasteet, kun hakkerit voivat suorittaa monimutkaisempia tehtäviä entistä tehokkaammin ja edullisemmin, lisäksi edistyneitä hyökkäyksiä on vaikeampi havaita ja vielä vaikeampi lopettaa (Kilpatrick, 2018). Tekoälyn nopea kehittyminen tulee Brundagen ym., (2018) mukaan aiheuttamaan uhkia, jotka voidaan jakaa kolmeen ryhmään (taulukko 1). Näistä kolmesta uhasta ensimmäinen ryhmä on digitaaliset uhat. Käytännössä tämä tarkoittaa, kun tekoälymenetelmät kehittyvät, niin samalla rikollisten käyttämät hakkerointimenetelmät tulevat entistä kehittyneimmiksi ja tehokkaimmiksi. Yritykset joutuvat tämän takia ottamaan huomioon uudenlaisten entistä tehokkaampien verkkohyökkäyksien mahdollisuuden, samalla kun he ottavat uusia tekoälyä hyödyntäviä sovelluksia käyttöön. Seuraava ryhmä on poliittiset uhat. Tämä kategoria ei suoraan koske finanssialaa, mutta finanssialan suuren yhteiskunnallisen vaikutuksen vuoksi finanssiala tai sen yksittäinen osa voisi olla myös rikollisten poliittisena motiivina. Finanssialan yrityksen keräävät asiakkaistaan suuria määriä dataa ja rikolliset voivat käyttää näitä tietoja omiin tarkoituksiinsa ja kohdentaa poliittisiin ryhmiin, mikäli he pääsevät dataan käsiksi. Kolmas ryhmä on fyysiset uhat. Kuten Brundage ym., (2018) toteavat; tekoälyä käytetään paljon jo tänä päivänä esimerkiksi dronejen ja muiden fyysisten laitteiden valvonnassa. Hakkeroimalla nämä järjestelmät, rikolliset pystyisivät aiheuttamaan yleistä turvallisuuden vaarantumista paikallista tai jopa maailmanlaajuisesti. Finanssialalla on digitaalisten sovellusten ja ohjelmistojen lisäksi käytössä myös fyysisiä laitteita aina tietokoneista ja maksupäätelaitteista, pankkiautomaatteihin ja kolikkotalletuslaitteisiin. Tästä syystä tekoälyyn liittyvät fyysiset uhat ovat läsnä myös finanssialalla.

TAULUKKO 1 Tekoälyn yleistymisen uhat (Brundage ym., 2018).

Tekoälyn yleistymiseen liittyvä uhka		
Digitaalinen	Poliittinen	Fyysinen
Hakkerointimetodit tulevat tekoälyn kehityksen myötä paljon kehittyneimmiksi ja tehokkaimmiksi. Hakkerit voivat hyökätä kokonaisiin verkkoihin entistä nopeammin manipuloimalla tekoälyjärjestelmiä.	Rikolliset voivat käyttää tekoälyä esimerkiksi valvontajärjestelmien manipulointiin tai analysoida massoista kerättyä dataa, jota hyödyntää ja kohdentaa poliittisiin ryhmiin.	Tekoälyjärjestelmät ovat jo käytössä dronejen ja muiden fyysisten laitteiden valvonnassa. Hakkeroimalla nämä järjestelmät rikolliset voisivat rikkoa yleistä turvallisuutta ja luoda jopa maailmanlaajuisia uhkia.

Aiemmissa tutkimuksissa nousi esiin tekoälyyn liittyvissä haasteissa myös yksityisyydensuojan rikkoutuminen. Näissä tapauksissa haitta kohdistuu usein finanssialan yritysten asiakkaisiin, identiteettivarkauksien, huijausten tai kiristysvaatimuksien muodossa. Yrityksille vaarana on mahdolliset sanktiot sekä maineen menetys. Datan vääriin käsiin päätymisellä voi olla todella tuhoisat seuraukset, kuten Isossa- Britanniassa kävi vuonna 2017, kun kiristyksen takia jouduttiin sulkemaan 16 sairaalaa (Jin, 2018). Treffisivusto Ashley Madisoniin kohdistuneen hakkeroinnin seurauksena sanotaan olleen myös tuhoisat seuraukset, kun useat hakkeroinnin kohteeksi joutuneet henkilöt tekivät itsemurhan (DailyMail, 2015).

Eräs merkittävä haaste yrityksille on dokumenttien, lomakkeiden ja muiden tärkeiden vanhojen paperilla olevien tietojen muuttaminen digitaaliseen muotoon. Lähes kaikki tekoälysovellukset ja -ohjelmistot tarvitsevat datan digitaalisessa muodossa ja mikäli ohjelmistosta halutaan saada sen tarjoama hyöty kokonaisuudessaan, sille pitäisi pystyä tarjoamaan riittävästi dataa menneiltä ajoilta. Azulay (2019) toteaakin, että yritysten pitäisikin muuttaa kaikki data ensiksi digitaaliseen muotoon, ennen kuin he rupeavat kehittämään tekoälysovelluksia tai ostavat niitä valmiina kolmansilta osapuolilta.

Finanssiala on tarkoin säännelty ja kuten Gill (2016) toteaa, uudenlainen tekoälyn tuoma teknologia voi luoda kokonaan uusia vaatimuksia valvonnalle tai uusien lakien muodostamiselle. Lakien luomisessa ja säännösten määrittelyssä ei aina pystytä toimimaan etukäteen ennustaen ja tekoälyn yleistyminen voi hankaloittaa epäselviä osa-alueita entuudestaan. Tekoälyä hyödyntävät lait-

teet eivät tunne eettisiä säännöksiä tai ihmismäistä moraalikäsitystä. Bostrom ja Yudkowsky (2011) kirjoittavat koneiden luomista moraalista ongelmista ja esittävät pohdintoja pankin asuntolainahakemuksista, joissa kone käyttää epäolennaisia tietoja päätöksenteossa. Tällaisia olivat esimerkiksi hakijan ihonväri tai asuinalueen postinumero. Aiemmin todettiin Javelosan (2017) sekä Huangin ja Rostin (2018) toimesta, että tekoälyn on osoitettu korvaavan korkeaa koulutusta vaativia työtehtäviä. Kouluttautuneilla ihmisillä on kuitenkin kouluttamattomia paremmat mahdollisuudet löytää uutta työtä menetetyn tilalle. Tekoälyn yleistymiseen liittyvänä haasteena Russell ym. (2015) mainitsevat, että yhteiskunta saattaa kohdata uudenlaisia haasteita koneiden viedessä joiltakin ihmisiltä työpaikan lopullisesti. Tekoälyn nähdään usein olevan yhteiskuntaa hyödyttävä ja tehostava asia, sekä nostavan tuottavuutta ja bruttokansantuotetta. Tästä huolimatta tekoälyyn liittyvät haasteet eivät yksilötasolla ole jokaisen kohdalla samanlaiset. Tekoäly luo myös paljon uusia työpaikkoja, mutta työnsä tekoälyn takia menettäneet eivät usein työllisty näihin työpaikkoihin, vaan menetys saattaa olla joissain tapauksissa koko työuran päättävä muutos.

Siukonen ja Neittaanmäki (2019) jaottelevat tekoälyyn liittyvät riskit neljään eri luokkaan (taulukko 2); ohjelmistotason, laitetason, eettisiin ja data-aineiston riskeihin. Ohjelmistotason riskeillä he tarkoittavat sitä, että tekoälysovellukset ja -ohjelmistot ovat aina ihmisten tekemiä. Tästä syystä ne voivat sisältää virheitä, joita rikolliset pystyvät hyödyntämään omiin tarkoituksiinsa. Laitetason riskeissä korostuu myös se, että laitteet ovat ihmisten tekemiä. Laitteisiin voidaan ujuttaa jo niiden tekovaiheessa erilaisia takaportteja tai troijalaisia, joiden avulla laitetta voidaan hallita etänä tai haluttu toiminto voidaan kytkeä päälle silloin kun sitä tarvitaan. Laitteisiin voidaan edellä mainitut asentaa myös jälkikäteen ihmisen toimesta. Data-aineiston riskillä Siukonen & Neittaanmäki (2019) tarkoittavat sitä, että tekoälysovellusten käyttämä data voi olla manipuloitua tai virheellistä, jolloin myös tulokset ovat väistämättä virheellisiä. Eettisillä riskeillä taas tarkoitetaan tekoälyyn liittyviä vastuukysymyksiä sekä yksityisyyteen liittyviä riskejä ja oikeuksia.

TAULUKKO 2 Tekoälyn riskitasojen lajittelu (Siukkonen & Neittaanmäki, 2019).

Riski:	**Mahdolliset seuraukset:**
Ohjelmistotaso	Ohjelmistot ovat ihmisten tekemiä, saattavat sisältää virheitä, joita rikolliset voivat hyödyntää.
Laitetaso	Takaportit ja troijalaiset, joilla voidaan kytkeä toimintoja päälle ja hallita laitteita etänä.
Eettinen	Vastuukysymykset, sekä yksityisyyteen liittyvät riskit.
Data-aineisto	Datan manipulointi tai virheellinen data johtaa virheellisiin tuloksiin.

Haasteita tuottaa myös ns. blackbox ratkaisua käyttävät tekoälysovellukset. Blackbox on eräänlainen automatisoitu päätöksenteon järjestelmä, jonka ratkaisut perustuvat koneoppimiseen big datasta saatavan tiedon pohjalta. Ongelmal-

liseksi sen tekee se, että blackbox ei paljasta syitä, joiden takia päätöksiin on päädytty (Adabi & Berrada, 2018). Ihmiset haluavat heitä koskevien koneiden tekemien päätösten olevan läpinäkyviä, lisäksi päätökset voivat olla epäreiluja tai vääriä, eikä niiden syytä saada selville. Koneoppiminen rakentaa päätöksentekojärjestelmät perustuen tietoihin, jotka kuvaavat ihmisen toiminnan digitaalisia jälkiä. Näin ollen mustanlaatikon mallit saattavat heijastaa ihmisten puolueellisuutta ja ennakkoluuloja. Monet kiistanalaiset tapaukset ovat jo korostaneet ongelmia päätöksenteon siirtämisessä blackboxin algoritmeille monilla arkaluonteisilla aloilla, mukaan lukien rikoksen ennustaminen, persoonallisuuspisteytys, kuvan luokittelu jne. (Guidotti ym., 2019). Blackbox-toteutukset ovat myös käytännössä ongelmallisia EU:n GDPR säädöksen suhteen. GDPR takaa yksityiselle henkilölle oikeiden tietää hänen omista tiedoistaan ja mitä hänestä tallennetaan ja mihin tietoja käytetään.

Hurjimmat riskit tai uhkakuvat tekoälyyn yleistymistä kohtaan liittyvät ns. supertekoälyyn, jolla voisi Turchin ja Denkenbergerin (2018) mukaan olla kyky pyyhkiä koko ihmiskunta pois maapallolta. Monet maailman rikkaimmista ja tunnetuimmista henkilöistä ovat myös kommentoineet supertekoälyyn liittyvistä mahdollisista vaaroista. Geist (2015) on koonnut eräiden tunnettujen henkilöiden ajatuksia seuraavasti: ”Sähköautoyritys Teslan johtaja Elon Musk tviittasi supertekoälyn olevan vaarallisempi kuin ydinaseiden. Tähän Bill Gates vastasi olevansa Muskin kanssa samaa mieltä, eikä ymmärrä miksi asia ei kaikkia ihmisiä huoleta ollenkaan. Kuuluisa fyysikko Stephen Hawking taas on todennut, että supertekoälyn kehittäminen voisi tarkoittaa koko ihmiskunnan loppua”. Tämän kaltaiset riskit ovat teoriassa mahdollisia, mutta tällä hetkellä ne ovat vielä toistaiseksi ennemminkin ennustuksia kuin todellisia riskejä. Supertekoälyä ei ole vielä käytössä missään muodossa, joten tämän tyyliset riskit tulevat ajankohtaisiksi aikaisintaan kymmenten vuosien päästä, eivätkä ne kosketa pelkästään finanssialaa, vaan koko ihmiskuntaa. Tästä syystä, aiheeseen ei tämän tutkimuksen empiirisessä osiossa tulla keskittymään laisinkaan.

3.3 Kirjallisuuskatsauksen pohdinta

Kirjallisuuskatsauksen pohjalta voidaan todeta, että aiempaa tutkimusta finanssialan tekoälyyn liittyvistä haasteista ja riskeistä on jo saatavilla. Tutkimuksissa esiintyneet haasteet ja riskit eivät kaikissa tapauksissa kohdistuneet pelkästään finanssialaan, vaan niissä oli osana myös yleisiä tekoälyyn liittyviä mahdollisia ongelmia. Tässä alaluvussa käydään lävitse tiiviisti kirjallisuuskatsauksen pohjalta löydettyjä haasteita (taulukko 3).

Tekoälyn nähtiin omaavan kyky viedä olemassa olevia työpaikkoja. Russell ym., (2015) totesivat tekoälyä käyttävien koneiden vievän työpaikkoja aloilta, joissa on matalasti koulutettua henkilökuntaa ja näille työntekijöille on vaikeampaa löytää uutta työtä tilalle, kuin korkeasti koulutetuille työntekijöille. Tekoälyn nähtiin myös voivan viedä työpaikkoja korkeasti koulutetuilta työntekijöiltä (Javelosa, 2017). Hieman saman suuntaisia ajatuksia toivat esiin myös

Huang ja Rust, (2018), joiden mukaan tekoäly korvaa analyyttisia taitoja vaativat työpaikat.

Kilpatrick (2018) sekä Brundage (2018) kirjoittivat tekoälyn yleistyvän käytön nostavan hakkeroinniksi joutumisen riskiä, sekä lisäävän yleisesti erilaisia tietoturvaongelmia. Samasta aiheesta kirjoitti myös Jin (2018). Hänen mukaansa tekoälyn takia on mahdollista, että yksityisyydensuoja rikkoutuu aiempaa herkemmin. Hän kirjoitti myös, että hakkeroinnin seurauksena vääriin käsiin joutuneet yksityiset tiedot tulevat johtamaan eri muotoisten kiristysten kasvaviin määriin. Azulayn (2019) mukaan asiakirjojen digitoimiseen liittyy suuria haasteita, sillä ennen kuin yrityksen voivat siirtyä täysimääräisemmin joka osa-alueella hyödyntämään tekoälyä, niin heidän tarvitsee muuttaa kaikki materiaalinsa paperilta digitaaliseen muotoon. Tekoälyn avulla pystytään tehostamaan monia toimintoja, mutta se tarvitsee päätöksen tekemiseen suuria datamääriä, joiden tulee olla saatavilla digitaalisessa muodossa.

Finanssiala on useissa maissa tarkkaan säännelty ala ja Gill (2016) kirjoitti tekoälyn luovan tarvetta kokonaan uudenlaiselle sääntelylle ja valvonnalle. Bostrom ja Yudkowsky (2011) kirjoittivat tekoälyyn liittyvistä moraalisista ja eettisistä ongelmista. Tekoälyä hyödyntävät koneet eivät tunne ihmismäisiä moraalikäsityksiä ja saattavat tehdä tästä syystä epäinhimillisiä päätöksiä. Eettisiä ongelmia sivuttiin myös Blackbox-tekniikalla toteutettujen sovellusten kohdalla Adabin ja Berradan (2018) sekä Guidottin ym., (2019) tutkimuksissa. He näkivät paljon mahdollisia epäselvyyksiä kyseistä tekoälytekniikkaa käytettäessä. Supertekoäly ja sen kyky tuhota koko ihmiskunta nähtiin myös suurena riskinä muun muassa Geistin (2015) sekä Turchinin ja Dengenbergerin (2018) tutkimuksissa.

Näitä edellä mainittuja maailmalta löydettyjä finanssialan tekoälyyn liittyviä haasteita ja riskejä (taulukko 3) tullaan pohtimaan ja vertaamaan tämän tutkimuksen empiirisen osion tuloksiin. Kirjallisuuskatsauksen löydökset ovat koottu useista maista eri puolilta maailmaa, mutta empiirisen tutkimuksen tulokset ovat kerätty ainoastaan Suomen finanssialan yrityksissä työskenteleviltä henkilöiltä. Myöhemmässä vertailussa pyritään löytämään samankaltaisuudet ja eroavaisuudet Suomen ja muun maailman välillä.

TAULUKKO 3 Tekoälyn haasteet ja riskit kirjallisuuskatsauksessa.

Tutkijat	Haaste/Riski
Huang & Rust, 2018.	Tekoäly korvaa analyyttisia taitoja vaativat työpaikat.
Javelosa, 2017.	Tekoäly korvaa korkeaa koulutusta vaativat työpaikat.
Russell ym., 2015.	Koneet vievät työpaikkoja matalasti koulutetuilta. Korkeakoulutetut löytävät helpommin uutta työtä menetetyn tilalle.

(jatkuu)

Taulukko 3 (jatkuu)

Kilpatrick, 2018. Brundage, 2018.	Riskit hakkeroinneille kasvavat ja tietoturva-haasteet lisääntyvät.
Jin, 2018.	Yksityisyydensuojan rikkoutuminen, Kiristysten riski kasvaa.
Azulay, 2019.	Vanhojen dokumenttien ja muun aineiston muuttaminen digitaaliseen muotoon.
Gill, 2016.	Uudenlaisia vaatimuksia sääntelylle ja valvon-nalle.
Bostrom & Yudkowsky, 2019.	Koneilla ei ole ihmismäisiä moraalisia tai eettisiä käsityksiä.
Adabi & Berrada. 2018. Guidotti ym., 2019.	Blackbox-tekniikkaan liittyvät haasteet
Turchin & Denkenberger, 2018. Geist, 2015.	Supertekoälyn mahdolliset, ihmiskunnalle tu-hoisat seuraukset.

4 EMPIIRINEN TUTKIMUS

Tässä luvussa käydään lävitse tutkimuksen empiirinen osuus. Luvun ensimmäisessä osiossa käydään mitä empiirinen tutkimus on ja miksi kyseinen metodi on valittu tämän tutkimuksen tutkimusmenetelmäksi. Luvun toisessa osiossa keskitytään siihen, kuinka empiirinen tutkimus on toteutettu.

4.1 Tutkimuksen taustat

Tutkimuksen empiirisessä osiossa tutkitaan, millaisia tekoälyn yleistymiseen liittyviä haasteita tai riskejä Suomen finanssialalla on havaittu. Luvussa kolme esitettiin kirjallisuuskatsauksen pohjalta, millaisia tekoälysovelluksia maailmalta löytyy finanssialan yhteydessä. Luvussa neljä esiteltiin millaisia haasteita ja riskejä maailmalta löytyy tekoälyyn liittyen, aiempien tutkimustietojen perusteella. Empiirisen tutkimuksen avulla selvitettiin miten vastaavat haasteet ja riskit koetaan Suomessa ja löytyykö niistä yhtäläisyyksiä kirjallisuuskatsauksen tapausten kanssa.

Empiirinen tutkimus erotellaan usein kahteen erilaiseen toteutustapaan, kvalitatiiviseen eli laadulliseen ja kvantitatiiviseen eli määrälliseen tutkimukseen. Tutkimusmetodit eivät ole toisiaan poissulkevia, vaan niitä on mahdollista käyttää päällekkäin toisiaan tukien. Määrällisessä tutkimuksessa nimensä mukaisesta pyritään saamaan mahdollisimman suuri määrä vastauksia tai aineistoa tutkimuksen pohjalle. Määrällinen tutkimus tuottaa usein vastauksena numeroita ja siinä käytetään tilastotieteen menetelmiä. Se ei kuitenkaan pysty kertomaan ilmiöiden syitä tai seurauksia, eikä vastaamaan esimerkiksi kysymykseen: miksi jotakin tapahtuu. Laadullinen tutkimusmenetelmä soveltuu hyvin tutkimaan uusia ilmiöitä, syitä tai mielipiteitä asioista, joita ei ole vielä kauheasti aiemmin tutkittu (Hirsjärvi ym., 2000). Laadullisessa tutkielmassa aineiston keräystapa on usein haastattelu ja otanta määrällisesti melko vähäinen. Aineisto ja haastatteluiden kohteet pyritään valitsemaan harkiten ja mahdollisimman tarkoituksenmukaisesti tutkittavaa aihetta ajatellen (Eskola & Suoranta, 1998). Tietojärjestelmätieteessä tutkittavat aiheet ovat yleensä uudehkoja

ja niissä on tärkeää pyrkiä ymmärtämään ilmiöitä ja kokonaisuuksia. Haastattelut ovat tärkeässä roolissa tiedon keruussa laadullisissa tutkielmissa (Myers & Newman, 2007). Näistä syistä johtuen, on perusteltua valita tämän pro-gradututkielman toteutustavaksi laadullinen, eli kvalitatiivinen tutkimus haastatteluiden avulla.

4.2 Empiirisen tutkimuksen toteutus

Tutkimus toteutettiin laadullisena, eli kvalitatiivisena tutkimuksena haastatteluiden muodossa. Tutkimukseen pyrittiin löytämään 3–7 kappaletta Suomen finanssialan yrityksissä työskentelevää henkilöä. Haastateltavien henkilöiden kohdalla ei ollut ennakkovaatimuksia tietystä ammattinimikkeestä tai työskentelyvuosien määrästä. Tarkoituksena oli löytää henkilöitä, jotka työskentelevät finanssialalla ja ovat jollakin tasolla tekemisissä tekoälyyn liittyvien asioiden kanssa työnsä puolesta. Lisäksi haastateltavien tuli olla asemassa, jossa he suoraan näkevät tekoälyyn liittyviä haasteita ja riskejä tai pohtivat ja miettivät näitä työhönsä liittyen. Osassa yrityksistä nimettiin suoraan haastatteluun parhaiten sopiva henkilö ja toisissa yrityksissä asiaa pohdittiin hieman pidempään. Tutkimusta varten haastateltavat pyrittiin etsimään myös finanssialan eri osa-alueilta, eli pankeista, vakuutusyhtiöistä ja rahastoyhtiöistä. Lisäksi ennakko-odotuksissa oli saada haastattelu Suomen finanssialaa valvovalta Finanssivalvonnalta, sillä heillä saattaisi olla tietämyksen lisäksi myös hieman erilaista näkökulmaa tekoälyn haasteisiin ja riskeihin, kuin mitä muilla finanssialan yrityksillä on.

Alun perin haastattelut oli tarkoitus saada tehtyä maaliskuun ja huhtikuun 2020 välisenä aikana. Maaliskuussa Covid-19, eli koronavirustilanne kuitenkin paheni maailmalla ja Suomessa niin paljon, että se vaikutti myös tutkimuksen haastatteluihin. Yksi jo sovittu haastattelutapaaminen jouduttiin perumaan kokonaan ja toisen haastateltavan kanssa siirrettiin haastattelua kuukaudella eteenpäin. Covid-19 aiheutti yrityksissä työskentelytapojen muutoksia, ruuhkautti asiakaspalvelulinjoja ja hankaloitti alkuun tapaamisten sopimisia. Lopulta tutkimusta varten saatiin tehtyä neljä haastattelua, yksi vakuutusyhtiön työntekijän kanssa, yksi Finanssivalvonnan edustajan kanssa, sekä kahden pankin työntekijän kanssa. Kaikki neljä haastattelua toteutettiin videohaastatteluina huhtikuun loppupuolen ja kesäkuun alkupuolen välissä vuonna 2020.

Haastattelumuotona toimi puolistrukturoidut teemahaastattelut. Strukturoidulla haastattelulla tarkoitetaan yleensä lomakemuodossa toteutettua haastattelua, jossa on valmiit kysymykset ja vastausvaihtoehdot. Avoin haastattelu taas on nimensä mukaan avoin haastattelutapahtuma ja kysymykset voivat vaihdella paljonkin haastateltavien kesken. Puolistrukturoitu haastattelu on edellä mainittujen välimuoto, siinä on strukturoitua väljempi rakenne, mutta kuitenkin ennalta-asetettuja kysymyksiä (Rubin & Rubin, 2005). Tämän tutkimuksen haastatteluissa oli kaikissa sama haastattelurakenne, jossa oli ennalta laadittuja kysymyksiä aihealueittain. Haastatteluissa oli kuitenkin tilaa esittää

lisä- tai välikysymyksiä ja haastateltavalla oli mahdollisuus kertoa vastaukset haluamallaan laajuudella. Valmiit haastattelukysymykset oli muodostettu pääosin kirjallisuuskatsauksen perusteella ja haastatteluaikaa oli varattu riittävästi, jotta haastattelurakenteesta voidaan myös poiketa ja aikaa jää lisäkysymyksille. Puolistrukturoitu haastattelumuoto on tähän tutkimukseen sopiva tutkimusmenetelmä, sillä valmiita kaikenkattavia kysymyksiä on etukäteen aiheesta mahdotonta laatia, eikä haastattelija osaa välttämättä kysyä kaikkea oleellista jokaiselta haastateltavalta ilman lisäkysymyksiä. Jokainen haastateltava sai alustavat kysymykset etukäteen noin viikkoa ennen haastattelua, jotta heillä oli hyvin aikaa valmistautua haastatteluun ja mahdollisesti selvittää joitakin tekoälyyn liittyviä seikkoja edustamiensa yritysten sisällä.

Haastateltaville etukäteen lähetetty kysymysrunko on jaettu kolmeen teemaan. Ensimmäisen teeman tarkoituksena on saada tietoa haastateltavan taustasta ja työstä. Kysymykset olivat seuraavanlaiset:

1. Kerro hieman itsestäsi, eli kuka olet ja mitä teet työksesi?

2. Kuinka kauan olet työskennellyt nykyisessä tehtävässäsi?

3. Kuinka kauan olet työskennellyt finanssialalla?

Ensimmäisten kysymysten tarkoitus on saada tietoa haastateltavasta henkilöstä, sillä kaikki haastateltavat työskentelevät eri yrityksissä eri tehtävissä. Kysymyksillä pyritään myös saamaan selville haastateltavien suhde finanssialaan ja tekoälyyn. Kysymysrungon toinen teema käsittelee sitä, millainen rooli tekoälyllä on haastateltavan henkilön organisaatiossa. Kysymykset olivat seuraavanlaiset:

1. Onko teidän yrityksessänne tekoälyä käytössä? Millä eri liiketoiminnan osa-alueilla?

2. Onko teidän yrityksessänne osa-alueita, joissa tekoälyä on aiemmin ollut käytössä, mutta sen käytöstä on myöhemmin luovuttu? Miksi siitä on luovuttu?

3. Onko yrityksessänne suunnitelmissa ottaa lähitulevaisuudessa tekoälyä käyttöön alueilla, joissa sitä ei ole aiemmin ollut käytössä?

4. Onko tekoälyn käytöstä ollut konkreettista hyötyä yrityksellenne? Millaista hyötyä ja millä liiketoiminnan osa-alueilla?

Toisen teeman kysymyksillä pyrittiin saamaan käsitystä siitä, missä yhteyksissä ja millaisia tekoälysovelluksia haastateltavien yrityksissä on käytössä tai suun-

nitelmissa ottaa käyttöön. Haastattelurungon kolmannessa osiossa kysymykset käsittelivät tekoälyyn liittyviä haasteita ja riskejä. Kysymykset olivat seuraavanlaisia:

1. Millaisin keinoin yrityksessänne pyritään tunnistamaan tekoälyn yleistymiseen mahdollisesti liittyviä haasteita tai riskejä?

2. Koetteko tekoälyn tuovan haasteita tai riskejä henkilöstöön liittyen (esimerkiksi rekrytointien tai koulutusten yhteydessä)?

3. Koetteko lakien tai säännösten tuovan haasteita tai riskejä tekoälyn yleistymiseen liittyen?

4. Koetteko haasteita tai riskejä Blackbox-menetelmällä toteutettujen tekoälysovellusten käytön yhteydessä?

5. Koetteko tekoälyn lisääntyvään käyttöön liittyvän moraalisia tai eettisiä haasteita tai ongelmia?

6. Useat finanssialan tarjoamat palvelut mielletään henkilökohtaista kanssakäymistä vaativiksi palveluiksi. Koetteko tekoälyn muokkaavan palveluita entistä kasvottomampaan suuntaan vai tekevän palveluista entistä henkilökohtaisempaa?

7. Koetteko tekoälyn mahdollisten virheellisten tulkintojen tuovan haasteita tai riskejä tekoälyn käyttöön liittyen? Millaisia?

8. Tekoälyn yleistyminen voi tuoda mukanaan uudenlaisia kohdennettuja hyökkäyksiä tai muuta entistä kehittyneempää rikollisuutta. Miten nämä seikat tulisi ottaa huomioon tekoälyohjelmistojen käytössä tai niiden käyttöönoton suunnittelussa?

9. Miten tekoälyn tekemien päätösten lopullinen vastuu mielestänne jakautuu? Onko vastuussa aina esimerkiksi tekoälyä käyttävä yritys, tekoälyn kehittänyt yritys vai onko jokainen tapaus erilainen?

10. Mitkä asiat koet suurimmiksi haasteiksi tai riskeiksi tekoälyn yleistyvän käytön suhteen?

11. Onko tunnistettuihin riskeihin varauduttu yrityksessänne tai onko niitä varten tehty suunnitelmia?

12. Onko sinulla muita asioita aiheeseen liittyvien, joita haluaisit tuoda vielä esille?

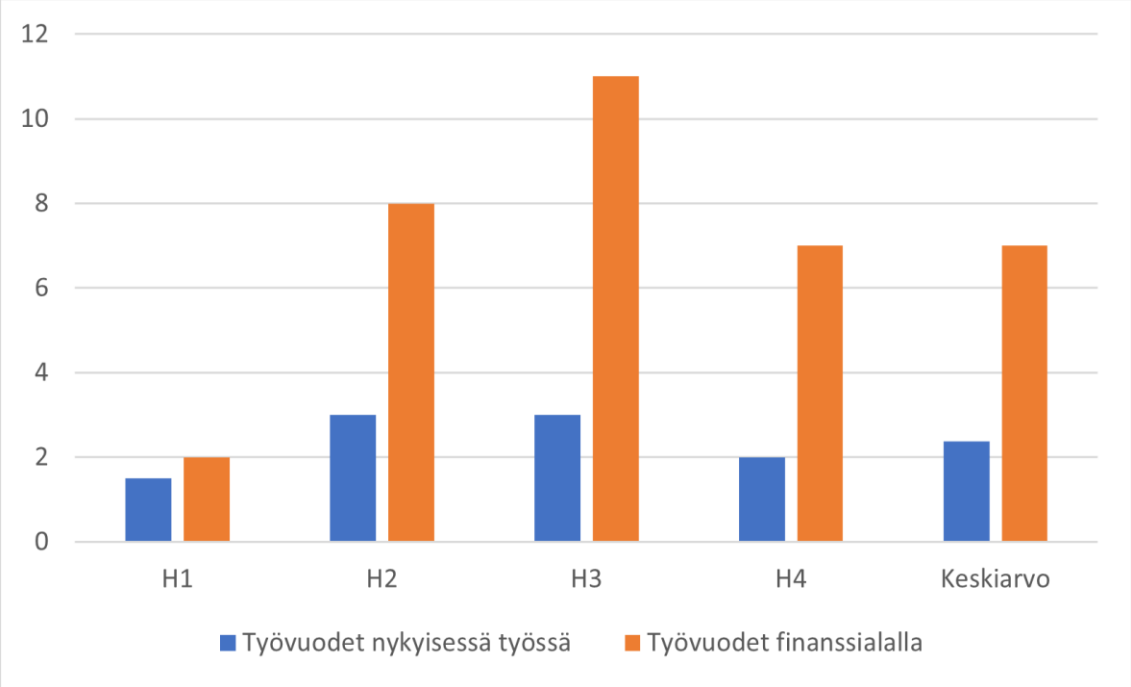
Kaikki haastattelut nauhoitettiin, jotta ne pystyttiin myöhemmin litteroimaan, eli puhtaaksi kirjoittamaan tarkasti sana sanalta tekstimuotoon. Litteroinnin jälkeen vastaukset käytiin tarkasti lävitse kysymys kerrallaan. Vastauksista pyrittiin löytämään samankaltaisuuksia ja ryhmittelemään ne Excel-taulukkoon. Vastausten litteroinnin pohjalta syntyi useita kymmeniä sivuja tekstiä. Tätä tekstiä on haastattelijan toimesta käyty useaan otteeseen lävitse ja pyritty löytämään vastauksista samankaltaisuudet ja eroavaisuudet.

Aineiston tarkempi lävitse käyminen toteutettiin yhdistelmänä deduktiivista ja induktiivista päättelymenetelmää. Aineiston läpikäyminen aloitettiin kysymys ja kysymysteemaosio kerrallaan. Ensimmäisen haastatteluosion vastaukset kirjattiin vain ylös, ilman sen enempiä vertailuja, sillä tämä osio koski haastateltavien taustatietoja. Toisen haastatteluosion kohdalla käsiteltiin haastateltavien yrityksissä käytössä olevaa tekoälyä. Tämän osion vastauksista pyrittiin löytämään yhtäläisyydet kirjallisuuskatsauksen alaluvun 2.3 (Tekoäly finanssialalla) kanssa. Kirjallisuuskatsauksessa kyseinen luku oli jaoteltu käytettävän metodin mukaan, mutta haastatelluissa ei erikseen kysytty tekoälyn metodia, vaan haastateltavat kertoivat vapaamuotoisesti, millaista tekoälyä on käytössä. Vastauksista pyrittiin löytämään kuitenkin käytetty tekoälysovellus vastaamaan jotakin kirjallisuuskatsauksen metodia. Tutkimuksen tuloksissa eroavaisuuksia ja samankaltaisuuksia vertailtaessa, on tutkimuksen luotettavuuden kannalta tiedostettava, onko empiirisen tutkimuksen ja kirjallisuuskatsauksen yrityksissä ollut ylipäätänsä käytössä samankaltaista tekoälyä. Haastattelurungon kolmasosio käsitteli samaa aihetta, kuin tämän tutkimuksen kirjallisuuskatsaukseen perustuva luku 3.2, tekoälyn haasteet ja riskit. Tämän osion kysymykset oli todella pitkälle koostettu niistä asioista, jotka kirjallisuuskatsauksessa nousi haasteiksi ja riskeiksi. Vastauksissa nähtiin melko suoraviivaisesti, mitkä samat asiat koettiin haasteiksi ja riskeiksi myös empiirisessä tutkimuksessa, ja mitä asioita ei vastaavasti koettu Suomessa haasteiksi ja riskeiksi. Löydetyt samankaltaisuudet ja eroavaisuudet merkattiin ylös, jotta niiden syitä pystyttiin selkeämmin tuloksissa pohtimaan.

5 EMPIIRISEN TUTKIMUKSEN TULOKSET

Tässä luvussa käydään lävitse empiirisen tutkimuksen haastatteluiden tulokset. Luvun alussa kerrotaan haastateltavien taustoista, luvun ensimmäisessä alaosiossa käydään lävitse, millaista tekoälyä haastateltavien yrityksissä käytetään ja luvun toinen alaosio käsittelee tekoälyn haasteita ja riskejä haastateltavien vastausten perusteella.

Haastattelut toteutettiin huhtikuun ja kesäkuun 2020 välisenä aikana ja niihin osallistui neljä henkilöä, neljästä eri yrityksestä. Haastatteluiden ennalta odotettu aika oli yksi tunti. Toteutuneiden haastatteluiden pituudet olivat 47, 56, 59 ja 64 minuuttia, joista muodostui haastatteluiden keskiarvolliseksi pituudeksi 56,5 minuuttia. Haastateltavat edustivat molempia sukupuolia, yhden ollessa nainen ja kolmen miehiä. Tarkkaa ikää ei haastateltavilta kysytty, sillä se ei tutkimuksen kannalta ole oleellinen tieto. Heidän arvioitu ikänsä oli noin 30–45 vuotta. Haastateltavien kokemusvuodet finanssialalla ja nykyisessä työtehtävässä, vaihtelivat suuresti (kuvio 6). Nykyisessä työtehtävässä lyhyin aika oli 1,5 vuotta ja pisin 3 vuotta ja keskiarvoksi nykyisissä työtehtävissä muodostui noin 2,4 vuotta. Haastateltavien työvuodet finanssialalla vaihtelivat myös paljon, lyhimmän ollen 2 vuotta ja pisimmän 11 vuotta, keskiarvon ollen 7 vuotta. Kaikkien haastateltavien koulutustausta oli ylempi korkeakoulututkinto. Haastateltavat ilmoittivat työskentelevänsä seuraavilla ammattinimikkeillä: kvantitatiivinen analyytikko, IT-asiantuntija/järjestelmävastaava, johtava digitalisaatioasiantuntija ja analyytikko.



KUVIO 6 Haastateltavien työvuodet.

5.1 Tekoälyn rooli yrityksessä

Tästä eteenpäin haastateltuihin henkilöihin viitataan seuraavilla lyhenteillä: VA (vakuutusyhtiö), PA1 (pankki), PA2 (pankki) ja FIVA (Finanssivalvonta). Haastateltavien kanssa on sovittu, että heihin tai heidän edustamiin yrityksiin ei viitata nimellä. Finanssivalvonnan kohdalla sovimme poikkeuksesta, sillä he edustavat valvovaa viranomaistahoa finanssialalla ja heidän suostumuksellansa lainauksissa saa olla heihin viittaava tunniste.

Tutkimuksessa kysyttiin haastateltavilta, minkälaisia tekoälyohjelmistoja heidän yrityksissään käytetään ja missä yhteydessä. Vastauksista käy ilmi, että tekoälyä käytetään Suomen finanssialalla useassa yhteydessä (taulukko 4). Huomioitava on kuitenkin se, että vaikka jotakin käyttötapaa ei ole jokaisen haastateltavan yhteydessä mainittu, niin tämä ei tarkoita, etteikö haastateltavan yrityksessä voisi olla myös kyseistä tekoälyä hyödyntävää ohjelmistoa käytössä. Tuloksissa on huomioitu vain ne seikat, jotka haastateltava on halunnut nostaa haastattelussa esille. Keskustelukanavissa käytettävät botit ns. chattibotit nousivat esille ensimmäisenä usean haastateltavan kohdalla. Chattibotit ovat usein finanssialan yritysten asiakkaille ensimmäinen kohtaaminen, kun heillä on aikomuksena tavoitella yrityksen asiakaspalvelua internetin kautta. Chattibotit osaavat ohjata asiakkaan oikeaan kanavaan ja näin ollen nopeuttavat myös asiakaspalvelin tehtäviä, sillä asiakaspalvelija tietää chattibotin ohjauksen perusteella paremmin, mistä asiasta asiakas mahdollisesti haluaisi keskustella. Tekoälyn koettiin parantavan myös asiakastyytyväisyyttä.

> PA1: ” kyllä sitä (tekoälyä) pyritään tuomaan vähän jokaiselle alueelle, mutta tottakai siitä pitää olla myös hyötyä, sen hyödyn ei tarvitse olla välttämättä suoraan liiketoimintaa parantavaa, vaan se voi sitä parantaa välillisesti, esimerkiksi paremmalla asiakastyytyväisyydellä”

Erilaisia puheen- ja tekstintunnistamista hyödyntäviä tekoälyohjelmistoja oli myös käytössä haastateltavien yrityksissä. Kuvantunnistamisen teknologioita vastaajat eivät sen sijaan maininneet käytettävän. Finanssialalla kuvantunnistuksella ei ainakaan vielä ole niin monia käyttötarkoituksia. Sitä hyödynnetään kyllä ainakin testaustarkoituksessa maailmalla joissakin vakuutusyhtiöissä vakuutuspetosten tunnistamiseen (Shang, 2018).

> PA2: ” puheen- ja tekstintunnistusta jonkun verran, kun halutaan palvella asiakkaita omalla äidinkielellä, niin tekoäly osaa sitten sen käytetyn kielen tunnistaa ”

> VA1: ” luonnollisen tekstin käsittelyä, siis semmoista, että kone käy joitain asiakirjoja läpi ja poimii sieltä tiedonpalasia ja taulukoi ne ”

> PA2: ” Sähköposteissa meillä on kanssa semmoista, että se tunnistaa tekstistä sellaisia avainsanoja ja niiden avulla se maili sitten ohjautuu oikeaan paikkaan ”

Haastateltavien yrityksissä oli tekoälyä käytössä myös sellaisissa yhteyksissä, joissa datan määrä on todella suuri ja sitä on ihmisen tästä syystä haastavaa käyttää yhtä tehokkaasti. Rahanpesun estäminen ja sen tunnistaminen nousivat esille tässä kategoriassa. Samoin myös tulevaisuuden ennustaminen kurssien ja tuottojen kohdalla mainittiin asiaksi, jossa datan suuri määrä on koneelle helpompaa käsitellä.

> PA1: ” No sitten on näytä alueita, missä se datan määrä on ihan järjetön, niin ei niitä ihminen oikein pysty samalla tavalla läpi käydä. Siis niin, kuin vaikka rahanpesun tunnistaminen tai ehkäisy, niissä läpikäytävää tietoa on tosi paljon, niin tekoäly on siinä yhteydessä iso apu ”

> PA2: ” Monessa missä koitetaan ennustaa jotakin, niin niissä on yleensä tosi paljon sitä lähdedataa, mitä käydään läpi tekoälyn avulla, just niin kuin erilaisten sijoitusten ja kurssien tulevaisuuden ennustaminen ”

Finanssialalla yrityksiä velvoitetaan tuntemaan asiakkaansa, lisäksi varsinkin pankkien tulisi tarkkailla rahaliikennettä ja raportoida epäilyttävät, mahdollisesti rahanpesuun viittaavat tapahtumat. Finanssivalvonta mainitsi myös haastattelussa käyttävänsä tekoälyä rahanpesun tunnistamiseen. Sen lisäksi, että he tekevät rahanpesun tunnistamista itse, niin he myös avustavat ja neuvovat valvottaviaan tarvittaessa. Suomessa valvonta kuuluu Finanssivalvonnalle, mutta heillä on paljon yhteistyötä myös muiden maiden viranomaisten kanssa. Tekoälyyn liittyviä yhteisiä Euroopan laajuisia järjestelmiä ei eri maiden valvovilla tahoilla vielä ole, mutta informaatiota vaihdetaan tiheästi ja myös suunnitelmia jonkin asteisista yhteisistä järjestelmistä on olemassa.

FIVA: ” Muualta Euroopasta, vaikka Saksasta, paikallinen valvoja saattaa lähettää semmoisia notifikaatioita. Sitten tässä notifikaatioprosessissa tieto viedään meidän järjestelmiimme ja rekistereihin robotiikan ja tekoälylajittelijan avulla ”

TAULUKKO 4 Tekoälyn käyttö

Tekoälyn käyttö:	**PA1**	**PA2**	**VA1**	**FIVA**
Chattibotit	X	X	X	
Asiakastyytyväisyyden parantaminen	X			
Puheentunnistus		X		
Tekstintunnistus		X	X	
Rahanpesun estäminen ja tunnistaminen	X	X		X
Kurssien ennustaminen	X	X		
Valvonnan tehostaminen				X
Notifikaatioprosessien tehostaminen				X

5.2 Poistunut tekoäly, tulevaisuuden tekoäly ja tekoälyn hyödyt

Tässä alaluvussa käydään niitä haastattelun kysymyksiä lävitse, jotka koskivat käytöstä poistunutta tekoälyä, tekoälyn hyötyjä, sekä tulevaisuudessa käyttöönotettavaa tekoälyä. Kysymykset on haastatteluissa esitetty, jotta voidaan verrata, onko haastateltavienyrityksissä ollut käytössä tai tuleeko olemaan samanlaisia tekoälysovelluksia, kuin kirjallisuuskatsauksen tutkimuksissa on todettu. Kysymykseen, onko jostain jo käytössä olleesta tekoälyä hyödyntävästä sovelluksesta luovuttu, saatiin kaikilta haastateltavilta saman suuntaisia vastauksia. Haastateltavat kertoivat, että eivät ole tietoisia oman yrityksensä kohdalla tekoälyn käytön lopettamisesta. Vastauksista kävi ilmi, että yrityksissä on kuitenkin ollut erilaisia tekoälyyn liittyviä epäonnistuneita pilottiprojekteja ja suunnitelmia, mutta ne eivät ole koskaan päässyt käyttöön asti. Osassa yrityksistä on oma yksikkönsä tekoälyn suunnittelua varten ja projekteja testataan paljon, jotta epäsopivat ohjelmistot saadaan karsittua jo ennen käyttöönottoa. Siitä huolimatta, että tekoälyä käytetään ja hyödynnetään jo paljon, niin vastauksista kävi ilmi, että tekoäly ei kuitenkaan ole vielä niin valtavirtaista tai vanhaa teknologiaa siinä mielessä, että sitä olisi keretty vielä poistamaan käytöstä.

Kyseinen kysymys on haastatteluissa esitetty, koska sitä kautta olisi mahdollisesti pystytty kertomaan jo toteutuneista tekoälyyn liittyvistä haasteista tai jopa varsinaisista riskeistä, mutta näitä ei vielä ainakaan ollut ensimmäistäkään tapahtunut. Voidaan myös miettiä syitä siihen, miksi ei vielä löydy epäonnistunutta tai epäsoveltuvaa poisvedettyä tekoälyä. Yksi syy voisi olla juuri suuri testauksen määrä ja lisäksi valvonta sekä rajoitukset varmasti myös vaikuttavat siihen, että huonoiten soveltuvat ohjelmistot eivät koskaan päädy käyttöön.

> FIVA: ” Moni on vielä melko aikaisessa vaiheessa tai hyvin rajatuissa pilottivaiheessa ja toki näistä paljon puhutaan, mutta sitten kun mennään vähän pinnan alle ja kun katsotaan, kuinka paljon on varsinaisesti tuotannossa, niin sitä on vielä aika vähän. En tunnista, että olisi viety käyttöön ja luovuttu. Mutta ehkä voisi olla semmoisia, että on mietitty voisiko työn tehdä tekoälyllä, mutta sitten tässä on vielä niin paljon haasteita, että ei ehkä ollakaan vielä tarpeeksi kypsiä hoitamaan niitä asioita tekoälyllä. Siihen liittyy niin paljon avoimia kysymyksiä vielä ”

> PA2: ” Meillä jonkin verran tuotetaan tuota omaa ohjelmistoa, niin siellä on ollut jotain semmoisia pilottihankkeita mitkä ei olo sitten koskaan päätynyt käyttöön. Mutta kyllä niitä yleisesti siis sillain testataan aika reilusti ja huolellisesti. Tarkoitus olisi, että ne sitten viimeistään siinä testivaiheessa päätyisivät hylätyksi. Sitten me ostetaan kyllä ulkopuolisiltakin, mutta siitä prosessista en kauhean tarkasti tiedä, mutta ei ole minun tiedossani, että olisi mitään jo käytössä ollutta tekoälysovellusta varsinaisesti kuopattu ”

> PA1: ” On ollut jotain epäonnistuneita projekteja, mutta en itse olo niistä kauhean tietoinen. Tai en ainakaan tiedä, että olisi ollut jo käytössä ja sitten myöhemmin olisi poistettu ”

Haastatteluiden seuraava kysymys koski suunnitelmia tulevaisuuden uusien tekoälysovellusten käytön suhteen. Vastaajat eivät olleet tietoisia uusista tekoälyohjelmistoista yrityksissään, eivätkä he tarkkoja tietoja tulevaisuuden suunnitelmista ymmärrettävästä syystä todennäköisesti kertoisikaan, sillä tietojen ei haluta päätyvän kilpailijoille, eikä haastateltavilla välttämättä olisi niistä kovin yksityiskohtaisesti lupaa puhua. Vastauksista voidaan kuitenkin päätellä, että tulevaisuuden finanssialalla tullaan kuitenkin ottamaan entistä enemmän uutta tekoälyä käyttöön myös uusilla liiketoiminnan alueilla, sitä mukaa kuin se yrityksissä koetaan kannattavaksi.

> VA1: ” Ei olo minun tiedossani mitään sellaista tiettyä aluetta mihin olisi tarkoitus ottaa, mutta yleisesti kyllä se varmasti tulee jokaiselle alueelle sitä mukaa kun se nähdään taloudellisesti kannattavaksi ”

> PA2: ” On meillä tuota omaa tuotantoa melko paljon. En ihan tarkalleen tiedä niiden suunnitelmista ihan kaikkea, tai välttämättä, että saanko niistä edes puhua. Niin sanotaan, että kyllä varmasti lähivuosina tulee enemmän ja enemmän uutta käyttöön ”

Haastatteluiden toisen osion viimeisessä kysymyksessä kysyttiin tekoälyn tuomia konkreettisia hyötyjä. Finanssivalvonnan kohdalla suurimmaksi hyödyksi

koettiin valvontaan ja monitorointiin liittyvät edut, sillä niiden kohdalla käsiteltävä datamäärä on usein valtavaa. Pankkien ja vakuutusyhtiön kohdalla esiin tulivat taloudelliset hyödyt, prosessien automatisoituminen ja toiminnan tehostuminen. Lisäksi tekoälyn koettiin olevan enemmänkin työntekijöiden tukena, kuin työntekijöiden korvaajana. Tämä oli suurehko ero kirjallisuuskatsaukseen verrattuna, sillä muun muassa Huang & Rust (2018), Javelosa (2017) ja Russell ym. (2015) kirjoittivat siitä, kuinka tekoälyllä on riskinä korvata ihmisten suorittamaa työtä. Suomessa sen sijaan vastaavaa riskiä ei juuri koettu.

> VA1: ” Taloudelliset hyödyt on ne isoimmat. Prosessien automatisointi ja taloudelliset hyödyt. Jos rahoitusta halutaan, vaikka johonkin uuteen projektiin ja nuo pystytään perustella hyvin, niin helpommin semmoiselle projektille näytetään vihreätä valoa ”

> FIVA: ” Kyllä se varmaan on erilaiset monitoroinnit, esimerkiksi toi rahanpesupuoli ja transaktioanalytiikka, siellä on ne volyymit niin valtavia, että eihän kukaan pysty manuaalisesti siellä tietenkään kaikkea tekemään. Kun eurooppalaisten kollegoiden kanssa juttelee, niin kyllähän tuo eniten taitaa olla toi rahanpesu ja rahanpesuntorjunta-analytiikka ”

> PA2: ” Paljon tekoäly nopeuttaa ja tehostaa toimintoja ja toki taloudellisesti myös monesti kannattavaa, mutta sen minkä itse huomannut, niin tekoälyn käytöstä on paljon myös sellaista yleistä tukea. Niin kuin ihan vaikka asiakaspalvelijoille, ne saa tekoälyltä paljon tukea ja sellaista lisäinfoa ja sen avulla ne pystyvät sitten myös asiakasta palvelemaan entistä paremmin ”

5.3 Koetut haasteet ja riskit

Haastatteluiden viimeisen osion kysymykset käsittelivät tekoälyyn liittyviä haasteita ja riskejä haastateltavien yrityksissä. Ennalta-asetettujen haastattelukysymysten joukkoon oli valittu osa kysymyksistä koskemaan sellaisia haasteita ja riskejä, joita kirjallisuuskatsauksen perusteella löydettiin Suomen ulkopuolelta. Näiden kysymysten vastauksia on jaettu X-MÄÄRÄÄN alalukuun. Viimeinen alaluku keskittyy haastateltavien suurimmiksi kokemiin haasteisiin ja riskeihin, sekä siihen kuinka näihin on varauduttu ja millaisia suunnitelmia niitä varten on tehty.

5.3.1 Haasteiden ja riskien tunnistaminen

Tässä alaluvussa käydään lävitse haastateltavien vastauksia, jotka koskivat heidän yrityksissään käytettyjä keinoja tekoälyyn liittyvien riskien ja haasteiden tunnistamiseen. Finanssivalvonnan vastauksesta käy ilmi, että asian yhteydessä tehdään paljon yhteistyötä Euroopan muiden valvovien viranomaisten kanssa. Haastateltava kertoi itse istuvansa eurooppalaisten viranomaisten työryhmissä, joissa mietitään teemaan liittyviä asioita. Finanssivalvonnan mukaan Euroopan

vakuutusvalvontaviranomainen (EIOPA) työstää tällä hetkellä vakuutusyhtiöitä varten ”supervision of machine learning algorithms guideline ”- ohjeistusta, josta valvottava näkee suoraan, mitä seikkoja tulee ottaa huomioon koneoppimisen sovelluksia käyttöönotettaessa, riskienhallinnan näkökulmasta. Lisäksi Euroopan valvoville viranomaisille on valmiita kysymyspaketteja, joista käy ilmi mitä tulisi kysyä finanssialan yritykseltä, joka aikoo ottaa käyttöön jotakin uutta tekoälyä toiminnoissaan. Myös muut haastateltavat korostivat riskienhallinnan tärkeittä haasteiden ja riskien tunnistamisessa. Haastateltava VA1 kertoi sääntelyn antavan kuitenkin melko laajat vapaudet toteutuksille, sillä osa säännöstelyistä on muotoiltu niin, että kaiken pitää olla hyvin toteutettu ja aivan surkeata toteutusta ei pääse sääntelyä noudattaessa edes syntymään. Haastateltava totesi, että jossakin toisessa asiassa säännöstely saattaa määritellä taas todella tarkoin esimerkiksi millaisia parametrejä tulee missäkin mallissa käyttää. Vastauksista kävi ilmi, että tekoälyyn liittyviä riskejä ja haasteita pyritään tunnistamaan etukäteen ja menetelmät ovat usein samoja tai saman tyylisiä kuin, minkä tahansa uuden teknologian käyttöönoton kohdalla. Kaikki vastaajat painottivat riskienhallinnan tärkeyttä ja vaikka haastateltavien kanssa ei keskusteltu syvemmin heidän riskienhallinnan menetelmistään, niin voidaan olettaa niiden olevan yleisiä käytössä olevia keinoja, joita myös kirjallisuuskatsauksessa käytiin lävitse, tämän tutkimuksen kolmannen luvun ensimmäisessä alaluvussa. Kuten Bouchaud ja Potters (2000) kirjoittivat, että riskien hallitseminen ja mittaaminen on yksi suurimmista huolenaiheista kaikessa nykyaikaisessa ihmisen toiminnassa, eikä finanssiala ole siinä poikkeus, niin tämän voidaan nähdä toteutuvan myös haastateltavien vastauksissa.

> FIVA: ” Näitä mietitään hyvin paljon riskienhallintalähtöisesti ja sitä kautta, jos joku valvottava yritys ottaa tekoälyä hyödyntävän ratkaisun käyttöön, niin mitä pitää ottaa huomioon. On laadittu yhteisesti esimerkiksi semmoisia check-listoja, mitä valvoja voisi ottaa huomioon ja kysellä ”

> VA1: ” Kyllä koko finanssiala on tosi compliance ja riskienhallinta orientoitunutta. Kaikki mitä tehdään, niin siinä on monta kerrosta riskienhallintaa ja vielä viranomaiset valvovat siihen päälle koko touhua. Monet sääntely jutut menevät sillain, että vaikka jossain sijoitusriskiraportoinnissa tavallaan se sääntely antaa aika paljon vapauksia niissä menetelmissä”

Kysymyksen vastauksissa lisämielenkiintoa toi se, että yksi haastateltavista edusti sääntelyä laativaa tahoa ja muut sääntelyä noudattavaa tahoa. Vastauksista käy selkeästi ilmi, että molemmat osapuolet ovat todella hyvin perillä siitä, mitä heiltä vaaditaan tekoälyn haasteiden ja riskien tunnistamisen suhteen. Yhteistyö koetaan vastausten perusteella tärkeäksi, niin valvovien kesken, kuin myös valvovan tahon ja valvottavien yritysten välillä. Haastattelija esitti Finanssivalvonnan edustajalle lisäkysymyksen koskien yhteistyötä: ”Mikäli yksittäinen pankki aikoo ottaa käyttöön jotakin uutta tekoälyä hyödyntävää sovellusta, niin pitääkö sen olla etukäteen yhteydessä finanssivalvontaan vai saako ottaa suoraan käyttöön?” Vastauksessa mainittiin, että lähtökohtaisesti pitää olla etukäteen yhteydessä. Mikäli ohjelmisto tulee kolmannen osapuolen toimit-

tajalta, niin ulkoistamista koskee omat säännöksensä. Mikäli sovellus koskee esimerkiksi maksamista, niin siihen vaaditaan erillinen esittely valvojalle ja useissa muissakin tapauksissa esittely on vähintäänkin suotavaa. Haastateltava kuitenkin korosti, että näissäkin tapauksissa yhteistyö on suuressa roolissa ja finanssialan yrityksillä on yleensä itsellään halu käydä uusia asioita yhdessä lävitse.

> FIVA: ” Lähtökohtaisesti kyllä pitää olla etukäteen yhteydessä. Se voi tulla kahta kautta, eli siinä saattaa olla ulkoistamisjärjestely, jos ostetaan jotain ulkoiselta kumppanilta tai tehdään yhteistyötä, niin ulkoistamista koskee aika tarkkaan erilainen sääntely. Se ei ole semmoinen formaali ennakkohyväksyntä sinänsä, mutta kyllä se prosessi on semmoinen, että niistä käytännössä etukäteen jutellaan ”

5.3.2 Koulutuksen ja säännöstelyn haasteet

Kirjallisuuskatsauksessa todettiin Huangin ja Rustin (2018) kirjoittavan siitä, että tekoäly korvaa analyyttisiä taitoja vaativia töitä. Javelosa (2017) kertoi työn menetysten kohdistuvan korkeasti koulutettuihin ja Gill (2016) totesi tekoälyn tuovan uusia vaatimuksia sääntelylle. Näiden kirjoitusten pohjalta tutkimukseen muodostettiin haastattelukysymyksiä, jotka koskivat henkilöstön osaamista, kouluttamista ja säännöstelyyn liittyviä haasteita. Tässä alaluvussa käydään lävitse näiden kysymysten vastaukset.

Vastauksissa oltiin sitä mieltä, että uutta osaamista vaaditaan jatkossa. Tekoälyn ei kuitenkaan nähty vievän merkittäviä määriä nykyisistä työpaikoista, ennemminkin luovan uusia ja tuovan pieniä haasteita jo olemassa oleviin. Osaavaa henkilökuntaa koettiin olevan saatavilla uusien rekrytointien kautta. Toisaalta osa vastaajista totesi, että joihinkin yksittäisiin alueisiin voi olla suoranainen työntekijäpula. Tekoälyyn nähtiin liittyvän koulutuksellisia haasteita, mutta niiden ei koettu olevan kovin vaikeasti selvitettävissä.

> PA1: ” On siinä kyllä omat haasteensa, ei mitenkään ylitsepääsemättömiä, mutta on kuitenkin. Työntekijöitäkin pyritään kyllä kouluttamaan, mutta sitten jos liian nopeasti asiat muuttuvat tai varsinkin moni asia samaan aikaan, niin ei se kaikille aivan helppoa tule olemaan ”

> PA2: ” Kyllä omanlaiset haasteensa tuo. Useasti on kuitenkin eri henkilöt, jotka ne käytettävät ohjelmistot ja laitteet suunnittelee, sitten eri henkilöt, jotka ne rakentavat ja lopuksi täysin eri henkilöt, jotka niitä päivittäisessä työssään käyttävät. Toki meilläkin on aina erilaisia talon sisäisiä koulutuksia eri juttuihin ”

> VA1: ” Kyllä varmasti semmoista uutta osaamista tarvitaan, mutta en minä tiedä onko se rekrytointi mielessä mitenkään mullistava ongelma. En osaa oikein sanoa onko pitkällä aikavälillä millainen trendi tämän suhteen. ”

Finanssivalvonta näki osaamiseen liittyvät haasteet myös riskienhallinnan kannalta. Vastauksessa mainittiin, että johdolla on lopulta vastuu, joten johdolla tulee olla myös riittävä ymmärrys ja tieto siitä mitä ollaan ottamassa käyttöön.

Johdon osaaminen on muutenkin tärkeässä roolissa, etenkin finanssialalla, jossa johdon osaamattomuuteen voidaan puuttua Finanssivalvonnan puolelta.

> FIVA: ” Johtohan viimekädessä vastaa, mutta se mitä finanssivalvonta on hyvin paljon nyt painottanut, on se johdon ymmärrys ja johdon tietoisuus, että jos tehdään tämmöisiä ratkaisuja, että otetaan tekoälyä käyttöön tai ulkoistetaan, niin ne pitää tehdä sillain, että siellä on tosi hyvin perattu se asia, ennen kuin se viedään johdon ratkaistavaksi.

Seuraava haastattelukysymys käsitteli lainsäädäntöön ja säännöksiin liittyviä haasteita ja riskejä tekoälyn yhteydessä. Finanssivalvonta on laatimassa säännöksiä, joten kysymys esitettiin heille myös toisella tavalla muotoillen, eli millaisia haasteita tekoälyn yleistyminen tuo säännösten laatimisen suhteen. Pääsääntöisesti vastaajat kokivat finanssialan sääntelyn hyväksi asiaksi, joka tekee alasta reilun, läpinäkyvämmän ja selkeän. Sääntelyn koettiin myös lisäävän byrokratiaa, mutta sen ei koettu olevan tekoälyn yhteydessä sen suurempaa tai monimutkaisempaa kuin alalla yleisesti minkä tahansa uuden asian yhteydessä. Finanssivalvonta koki sääntelyn yhteydessä haasteeksi datan määrän tai oikeanlaisen datan ja kuinka estää, että ei synny sen perusteella asiakaskohtaista syrjintää. Esimerkkinä haastateltava mainitsi vakuutusalan, jossa asiakkaalla on todellisuudessa parempi tieto omasta itsestään, kuin mitä vakuutuksen antajalla on. Ongelmia voisi muodostua, jos kaikki tieto olisi saatavilla ja sen takia vakuutusta tarvitseva ei vakuutusta saisi. Haasteellisia asioita, joita Finanssivalvonnassa pohditaan ja otetaan huomioon. Kasvava tiedon määrä ei saisi johtaa yksilöä syrjivään lopputulokseen.

> PA2: ” Ehkä se hieman lisää paperityötä ja byrokratiaa, kun kaikki on tarkasti säänneltyä. Toki se on kaikkien osapuolten kannalta reilua, että on selkeähköt säännöt ”

> VA1: ” Kyllä siinä on monta tarkistuskierrosta, mitä pitää käydä, just sääntelyyn liittyen ja sitten tavallaan, kun niitä tekoälyn sovelluksia ei kaikilla yhtiön osa-alueilla just vielä ole, niin jossain se on se ensimmäinen ja silloin siinä on juuri tätä uutuuden ongelmaa ”

> FIVA: ” Se mistä valvoja on erityisen huolissaan ja kiinnostunut, on tämä datan eettinen käyttö yhdistelmänä eri palveluissa. Ja mitä datalähteitä on kenties ookoo käyttää ja, että onko se koulutus ollut sitten oikeellista, että se ei tuotakaan vääristymiä. Ehkä minä juuri haasteeksi sanoisin just sitä, että tekoälyratkaisu tekee jotain mikä voisi johtaa syrjintään tai sitten myös se, ettei pakotettaisi liialliseen dataan käyttöön. Tällä tarkoitan sitä, että ei esimerkiksi sanottaisi, että sinä voit saada lainaa, jos annat meille nämä ja nämä datat ”

Finanssialaan liittyvän tekoälyn säännösten valvonta ei rajoitu ainoastaan Finanssivalvontaan. Tekoälyyn liittyy myös tietosuojallisia- sekä yhdenvertaisuuskysymyksiä, ja näihin liittyvät haasteet ja riskit kohdistuvat eri tahoihin. Tälläkin osa-alueella viranomaiset tekevät toistensa kanssa tiivistä yhteistyötä, ratkoessaan kysymyksiä ja laatiessaan säännöksiä.

> FIVA: ” Meillä se näkyy valvonnassa, että meillä on hyvin tiivis yhteistyö tietosuoja- ja yhdenvertaisvaltuutetun kanssa. Nämä kysymykset menevät myös usean eri viranomaisen tontille, että se ei ole vain Finanssivalvonta. Kaikista tärkeimmät ovat nämä yksilöiden oikeuksia suojaavat pelisäännöt. Kun tässä ollaan myös perusoikeudellisissa kysymyksissä kiinni, tämmöisissä yhdenvertaisuus ja syrjimättömyys kysymyksissä, niin ne ovat yhteiskunnallisesti tärkeitä”

Tekoälyyn liittyvät riskit voivat konkretisoitua taloudellisina tappioina tai pahimmissa tapauksissa ihmishenkien menetyksenä. Tästä syystä riskejä ja niihin suhtautumista on pohdittava ja säänneltävä etukäteen ennen kuin jotakin tapahtuu. Etukäteissuunnittelua on tehtävä niin finanssialalla, kuin muillakin kriittisillä aloilla, joissa tekoälyä on käytössä. Finanssivalvonnan vastauksista käy ilmi, että nämä seikat ovat Euroopan tasolla mietinnässä ja parhaimpia vaihtoehtoja haetaan yhteistyön avulla.

> FIVA: ” Tekoälyn uudet riskit voi olla sitä, että jos tapahtuu jotain ennakoimatonta ja nyt kun Euroopan komissiolla on lausunnoilla nämä tekoälyä koskevat sääntelyaloitteet. Niin siellä on nostettu esiin kysymyksenä, että pitäisikö olla lisäsääntelyä korkean riskin tekoälysovelluksille ja siellä mainittiin muun muassa terveydenhuolto ja älyliikenne ”

5.3.3 Blackboxin riskit, sekä moraaliset ja eettiset haasteet

Kirjallisuuskatsauksessa käsiteltiin Adabin ja Berradan (2018), sekä Guidottin ym. (2019) kirjoittamia tutkimuksia blackbox-tekniikalla toteutettujen tekoälysovellusten riskisyydestä. Kyseisestä aiheesta esitettiin kysymyksiä myös haastateltaville. Vastauksista voidaan suoraviivaisesti todeta, että Suomen finanssialalla blackboxit eivät tuota haasteita tai riskejä. Tämä johtuu yksinkertaisesti siitä, että niitä ei käytetä. Päällimmäisinä syinä tähän on lainsäädäntö ja säännökset. Osa vastaajista kuitenkin totesi, että blackboxien avulla voitaisiin mahdollisesti saada hyviäkin tuloksia, mutta tuloksiin johtaneita syitä olisi lähes mahdotonta raportoida tarvittaessa viranomaisille tai asiakkaille. Lyhyesti voidaan todeta, että blackboxin metodeja hyödyntävät tekoälyohjelmistot eivät sovellu finanssialalle, ainakaan Suomessa.

> VA1: ” Vaikka ne ei yleisesti sovellu, niin se vähän riippuu tapauksesta. Monet jutut varainhoitotoiminnassa pitää raportoida, joko viranomaisille tai asiakkaalle. Niiltä tulee yleensä kriteerit, että millaista raportointia ne haluavat ja millä menetelmillä. Sitten jos ne kriteerit käytännössä estää tuollaiset blackbox menetelmät, niin ei niitä silloin voi sitten käyttää ”

> PA1: ” Maailmalta olen lukenut tai kuullut näistä, että on blackbox hylännyt kaikki lainahakemuksen, jos ne hakijat on asunut jollakin tietyllä postinumeroalueella. On niitä blackbox juttuja varmaan jossakin käytössä, mutta meillä ei ole. Eikä ne täällä meillä oikein ole edes mahdollisia ”

Finanssivalvonta korosti blackbox-kysymyksen yhteydessä, että aina pitäisi pystyä perustelemaan päätökseen johtanut prosessi. Toinen tärkeä, huomion

arvoinen kommentti oli, että yritys ei vastuuta pysty ulkoistamaan. Vaikka ohjelmiston tai laitteen valmistus olisi ulkoistettu, niin sitä käyttävä yritys on vastuussa siitä, että he noudattavat säännöksiä ja lakeja.

> FIVA: ” Niin ainahan se lähtökohta on se, että vastuuta ei voi ulkoistaa. Jos nyt joku sijoituspalveluyritys ottaisi tämmöisen palvelun käyttöön, niin eihän ne voi sitten sanoa, että se oli se algoritmi, että ei se oltu me, että emme me vastaa tästä. Se on aina, että sinä vastaat myös sinun ulkoistuksistasi, että vastuuta ei voi ulkoistaa”

Haastattelun seuraava kysymys käsitteli tekoälyn yleistymisen mukana tulevia mahdollisia moraalisia tai eettisiä haasteita, joista kirjallisuuskatsaus osiossa kirjoitti muun muassa Bostrom ja Yudkowsky (2011). Useassa vastauksessa nousi esille maksutietojen käyttömahdollisuuksien moraalisuus, sillä korttitiedoista on johdettavista todella paljon informaatiota yksityisen henkilön arkirutiineista ja paheista, aina sijaintitietoihin asti. Tekoälyyn koettiin haastateltavien puolesta liittyvän eettisiä ja moraalisia haasteita, mutta ne nähtiin osittain koskevan tekoälyä itseään, ja niiden koettiin olevan enemmänkin koko yhteiskuntaa koskevia ongelmia, eikä niinkään pelkästään finanssialaa koskevia.

> VA1: ” No kyllä ihan yleisellä taholla tekoälyn yleistyminen, se korjaa, luo ja tuhoaa työpaikkoja. Niin onhan se sillain ihan yhteiskunnallinen ilmiö ja niin kuin tietysti ja varmaan poliitikkojen pitää huomioida jollain tavalla. En minä mihinkään suuriin eettisiin haasteisiin ole itse ainakaan törmännyt ”

> FIVA: ” Niitä on aika paljonkin, ja ehkä just se, että mitä tietoa velvoitetaan antamaan. Nythän on tietysti uutta sääntelyä voimassa, joka mahdollistaa nämä tämmöiset tilitietopalvelut, eli käyttäjän suostumuksella kolmasosapuoli vois katsoa hänen maksutiliänsä ja tehdä sen avulla johtopäätöksiä”

> PA1: ” Ensimmäisenä tulee mieleen korttitiedot, siis missä korttia käytetään ja mitä ostetaan. Siitä saa paljon tietoa ja periaatteessa niistä voisi väärissä käsissä olla myös haittaa. Sitten ihan yleisesti tekoälyn yhteydessä, niin onhan aina nämä esimerkki kysymykset ilmoilla, eli juuri ne, että itseohjautuva auto, niin miten se tekee päätöksen, jos pitää kolarissa valita osuuko vanhukseen vai lapseen ”

5.3.4 Palveluiden muokkaantuminen ja virheelliset tulkinnat

Finanssialan palvelut mielletään usein henkilökohtaista kanssakäymistä vaativiksi tapahtumiksi (Mehrotra, 2019). Seuraava haastattelukysymys koski sitä, koetaanko tekoälyn yleistymisen muokkaavan alaa entistä kasvottomampaan suuntaan vai pystyykö se tarjoamaan entistä henkilökohtaisempaa palvelua asiakkailleen. Vastauksista ei muodostunut yhtä yleistettävää kantaa, vaan jokainen vastaaja näki asian molemmat puolet. Palveluita on ohjattu kasvottomampaan suuntaan digitalisaation myötä, sekä kustannussäästöjen takia, mutta vastauksissa koettiin kuitenkin, että tekoäly auttaa työntekijöitä tarjoamaan entistä parempaa ja henkilökohtaisempaa palvelua. Aiempien kysymysten kohdalla todettiin kirjallisuuskatsauksen pohjalta tekoälyn uhkaavan viedä ihmis-

työnä suoritettavia työpaikkoja, mutta Suomessa asiaa ei nähty aivan niin uhkaavana. Tämän kysymyksen kohdalla on taustalla havaittavissa hieman samaa syytä kirjallisuuskatsauksen ja empiirisen tutkimuksen tulosten eroihin. Suomessa tekoälyä ei koeta niinkään työpaikkoja vievänä uhkana, vaan työntekijän työskentelyä tehostavana ja tukevana teknologiana. Tämä vaikuttaa myös siihen, että haastateltavat kokivat tekoälyn mahdollistavan entistä yksilöllisemmän palvelun joissakin tapauksissa.

> PA2: ” Hieman kaksipiippuinen asia. Näkisin, että riippuu paljon mitä aluetta tarkastellaan. Meillä moni asia on koitettu ohjatta sillain, että saisi sen infon myös ilman sitä ihmiskontaktia, eli asiakaspalvelua. Tulee kyllä palautetta, varsinkin vanhemmilta ihmisiltä, että jokin asia on hankalampaa kuin aiemmin. Sitten taas tekoälystä kyllä paljon sellaista hyötyä meidän työntekijöillemme ja itse koen, että sen avulla pystymme sitten kyllä palvelemaan asiakasta entistä paremmin ja pohtimaan mikä vaihtoehto olisi paras juuri kyseiselle asiakkaalle ”

> FIVA: ” En ole ihan varma, että muokkaako se tekoäly nyt niinkään sitä kuluttajarajapintaa. Vai muokkaako se enemmän yrityksen sisäisiä toteutustapoja sen sijaan, että tekeekö luottopäätöksen ihminen vai sen tekeekin tekoäly tai robotti. Ylipäätään tämä digitaalinen kehitys on ohjannut siihen, että pyritään ohjaamaan ihmisiä itsepalvelukanaviin ja digitaalisiin kanaviin. En näe, että se olisi nimenomaan tekoäly, joka tätä on muokannut, vaan ihan niin kuin puhtaasti, että on haettu kustannussäästöä digitalisaation kautta, olkoon se sitten mikä tapa tahansa ”

> VA1: ” No varmaan tekoälyä käytetään paljon tällaisessa asiakkaan tuntemisessa, millä pystytään sitten ohjaamaan myyjiä. En minä näe, että tällainen ihmisen tekemä myynti tulisi mitenkään lakkaamaan. Näen, että tekoäly olisi siinä sitten enemmän niin kuin tukena. Kyllähän on myös yhtiöitä, jotka myyvät tuotteita pelkästään vaan verkon yli, mutta en usko, että ne riittävät kaikille kuitenkaan ”

Haastattelun seuraava kysymys koski tekoälyn mahdollisia vääriä tulkintoja. Vastauksissa oltiin lähes yhtä mieltä siitä, että väärät tulkinnat ovat mahdollisia ja luovat omat haasteensa. Tekoälysovellukset ovat ihmisten tekemiä ja virheet ovat inhimillisiä. Myös tulkinnat voivat syystä tai toisesta poiketa siitä, mitä on aiemmin odotettu, eikä saisi alkaa luottamaan pelkästään tekoälyyn, vaan päätöksiä tulisi myös tarkastaa. Tämän kysymyksen vastauksissa kaikilla haastateltavilla oli melko samankaltaisia ajatuksia siitä, että tekoälyn tekemät väärät tulkinnat koetaan yhdeksi suurimmista tekoälyyn liittyvistä riskeistä ja haasteista.

> VA1: ” Tämmöinen malliriski, niin kuin usein ajatellaan finanssialalla. Se tulee huomioida ja siihen sisältyy semmoinen, että tavallaan jos joku malli antaa yksinkertaisen vastauksen johonkin ongelmaan, niin sitten siihen aletaankin luottaa ehkä vähän liikaa siihen vastaukseen, jos ei tunneta niitä sen menetelmän rajoitteita hirmu hyvin ”

> PA1: ” Kyllä aina on vaara, että tulkinnat eivät ole sellaisia kuin on alun perin haluttu tai toivottu. Tekoälykin on ihmisen luomaa, niin virheitä ja väärinymmärryksiä voi sattua ja varmasti sattuukin. Tekoälyn antamia tuloksia tai päätöksiä olisi varmasti hyvä tarkistaa ja käydä lävitse aina silloin tällöin, vaikka kaikki näyttäisi

olevan kunnossa, niin aina hyvä tarkistaa ja vähän kyseenalaistaa. Sitten jos kaikki onkin kunnossa, niin ymmärretään kuitenkin paremmin ne syyt, minkä takia kaikki oli kunnossa ”

FIVA: ” Toi on just se iso riski ja ehkä minä tästä juuri painottaisin, että se on niin A ja O se koulutusdata ja sen laatu. Jos nyt kouluttaa vääristyneellä datalla, niin ei sieltä voi tulla muuta kuin vääristyneitä lopputuloksia”

5.3.5 Tekoälyyn liittyvä rikollisuus ja vastuun jakautuminen

Tässä alaluvussa käydään lävitse haastateltavien vastauksia kysymyksiin, koskien tekoälyyn liittyvään rikollisuuteen ja lopullisten vastuiden jakautumisen. Tekoälyä hyödyntävät rikolliset koettiin osittain riskiksi, mutta vastauksista kävi myös ilmi, että asiaa pohditaan etukäteen ja sitä lähestytään jo kehitysvaiheessa riskienhallinnan keinoin. Tämän kysymyksen vastauksessa oli havaittavissa hieman samankaltaista ajatusta, kuin moraalisten ja eettisten haasteiden kohdalla. Toisin sanoen, tekoälyn mukanaan tuoma uudenlainen rikollisuus koskettaa finanssialaa, mutta sitä ei nähdä myöskään vain finanssialan ongelmana, vaan koko yhteiskunnan.

VA1: ” Sen tekoälysovelluksen käyttäjän pitää tietysti ymmärtää ne riskit mitä ottaa siinä, kun alkaa käyttämään sovellusta. Mikä se sovelluksen toiminnan kriittisyys on, että onko siinä riittävän luotettavat varajärjestelmät. Jos hankkii itsestään ajavan auton niin kyllä siinä pitää ymmärtää, että vaikka sensoreita pystytään häiritsemään ”

FIVA: ” Tämä ei sinänsä lisää sääntelyä, mutta ehdottomasti pitää ottaa huomioon, että kyllähän rikollisetkin tulee koko ajan teknologisesti edistyneemmäksi ja pyrkivät käyttämään juuri tekoälyä hyödyksi heidän hyökkäyksissään. Kyllä tämä on aina ollut sellaista kilpajuoksua rikollisten ja hyvien toimijoiden välillä tämä tietoverkkomaailma, mutta niinhän se on aina ollut. Sitten, kun teknologia kehittyy, niin tulee uusia keinoja niin suojautujille kuin hyökkääjille, ja samanlailla tekoäly tuo molemmille uusia keinoja”

PA2: ” Rikolliset pyrkii varmasti aina olemaan teknologisen kehityksen mukana. Vaikea nähdä, etteikö tekoäly olisi myös heillä entistä enemmän käytössä ”

Haastatteluiden seuraavassa kysymyksessä kysyttiin tekoälyyn liittyvistä vastuista. Kenellä lopulta on vastuu tekoälyn tekemistä päätöksistä? Tekoälyn valmistajalla, tekoälyä käyttävällä yrityksellä vai onko jokainen tapaus erilainen? Jälkikäteen ajatellen, haastattelija olisi voinut muotoilla kysymyksen hieman eri tavalla, sillä tämä kysymys on haastattelun ainoa kysymys, johon periaatteessa on yksi oikea vastaus. Kysymyksen taustalla oli ajatus siitä, että voiko lopullinen vastuu tuottaa ongelmatilanteissa ongelmia, mutta kaikki haastateltavat olivat yksimielisiä siitä, että vastuunkantajan löytäminen on useimmissa tapauksissa finanssialalla helppoa. Finanssivalvonta tiivisti asian niin, että vastuuta ei voi ulkoista, vaikka yrityksillä voikin olla kolmannen osapuolen kanssa keskinäisiä sopimuksia.

FIVA: ” Jos katsoo asiaa finanssialan näkökulmasta, niin vastuu on aina sillä pankilla tai vakuutusyhtiöllä, joka ratkaisun on ottanut käyttöön. He vastaavat tietysti viranomaisille. Mutta heillä on varmasti paljon vastuulausekkeita heidän sisäisissä sopimuksissaan, että mikä on vastuu teknologian toimittajan ja pankin välillä. Korvauslausekkeita ja semmoisia, mutta se juridinen vastuu käyttäjiä kohtaan on pankilla ja yhtä lailla pankki vastaa sitten viranomaisia vastaan, että nyt meni pieleen, mutta sitten voi olla juuri erikseen sopimusketjuissa ne vahingonkorvausvastuut”

5.3.6 Suurimmat haasteet ja riskit, sekä niihin varautuminen

Tässä osiossa käydään lävitse haastateltavien vastauksia kysymyksiin, jotka koskivat heidän itsensä suurimmiksi kokemiksi haasteiksi tai riskeiksi, sekä mahdollisia suunnitelmia näihin varautumiseen. Haastattelurungon tämän osion seuraavassa kysymyksessä haastateltavilta kysyttiin minkä tai mitkä asiat he itse kokevat suurimmiksi haasteiksi tai riskeiksi yleistyvän tekoälyn käytön yhteydessä. Vastauksissa tuli ilmi johdon osaaminen, datan kerääminen, tietovuodot, uudenlaisen osaamisen vaatiminen sekä tiedon avoimuus ja saatavuus. Johdon osaamisen voisi nähdä kuuluvan samaan kategoriaan muun sellaisen tekoälyyn liittyvän osaamisen kanssa, jota käsiteltiin kirjallisuuskatsauksessa. Se ei sitä kuitenkaan ole, sillä kirjallisuuskatsauksessa osaaminen liittyi lähes poikkeuksetta työntekijöiden osaamiseen ja taustalla oli uhka työpaikkojen menettämisestä tekoälylle. Haastatteluissa esille tullut huoli johdon osaamisesta taas liittyy siihen, onko johto tarpeeksi ymmärtäväinen ja kykenevä tekemään päätökset, joko koskien tekoälyn käyttöönottoa tai tekoälyn antamien tulosten yhteydessä. Tämä huoli koski erityisesti Finanssivalvontaa ja heidän haastateltava myös mainitsi, että he ovat joutuneet puuttumaan joidenkin yritysten kohdalla uusien johtajien aloittaessa työnsä, sillä uudella toimitusjohtajalla ei ole ollut finanssialakohtaista vaadittua osaamista, vaikka muuten hän olisikin ollut menestyvä ammattijohtaja. Datamäärät, datan kerääminen ja sitä kautta tietovuodot olivat asioita, jotka aiheuttivat huolija jollakin tasolla jokaisessa vastaajassa.

PA1: ” Ehkä semmoinen koko yhteiskunnan muuttuminen, ei niinkään pelkkä finanssiala. Samoin kuin digitalisaatio on muokannut tosi paljon useita eri aloja kokonaan uudenlaisiksi, niin tekoäly voisi tehdä saman. Kun moni asia muuttuu, niin vaaditaan uudenlaista osaamista, tai ei pelkästään osaamista vaan ihan uusien kokonaisuuksien ymmärtämistä. Sitten jos muutos on tarpeeksi nopea, niin monelle varsinkin sellaisille, jotka ovat kerenneet tehdä töitä samoilla menetelmillä jopa kymmeniä vuosia, niin heidän pitäisikin opetella kokonaan uutta”

VA1: ” Varmasti isoin yksittäinen haaste on juuri tuo datan kerääminen ja se, että ihmiset ja yritykset eivät ymmärrä miten paljon heistä tietoa kerätään eri paikkoihin. Ja sitten se luo sen riskin, että kaikilla yrityksillä alkaa olla merkittävät henkilötietovarannot, niin ei se vaan tilastollisesti ole mahdollista, että ne kaikki pystyisivät pitämään tällaista arkaluontoista tietoa luottamuksellisesti. Näitä tietovuotoja kyllä tapahtuu. Minä uskoisin, että se on yksi tämmöinen ehdottomasti suurimpia haasteita ja riskejä, koska se toteutuukin ihan jatkuvasti”

PA2: ” Sanoisin, että minun mielestäni ne liittyvät tietoon ja tiedon määrään. Meillä on GDPR:ää ja muita säännöksiä, jotka velvoittavat tekemään ja pyydettäessä jakamaan tiettyjä asioita, mutta tietoa on paljon. Se voi jossain vaiheessa mennä siihen, että se kaikki tieto ei enää näyttäydy niin avoimena. Data voi joutua myös vääriin käsiin ja aiheuttaa sitä kautta ongelmia. Uskon, että suurimmat haasteet ja riskit todentuvat jollakin tavoin dataan liittyen ”

FIVA: ” Minä sanoisin, että johdon tietoisuus ja johdon ymmärrys. Asian riittävän kattavalla, mutta ymmärrettävällä tavalla kuvaaminen johdolle, ennen kuin johto tekee näitä olennaisia päätöksiä jonkun ratkaisun ottamisesta käyttöön ”

Haastattelurungon viimeinen kysymys koski tekoälyn haasteisiin varautumista ja onko siihen tehtynä erillisiä suunnitelmia. Vastauksista kävi ilmi, että Suomessa asiat ovat varautumisen ja suunnittelun kannalta hyvällä mallilla. Säännökset ja lait, yhdessä riskienhallinta käytänteiden kanssa ohjaavat yritykset pohtimaan ja varautumaan myös ongelmakohtiin. Harvalla haastatteluihin osallistuneella oli kuitenkaan erikseen tekoälyn riskeihin liittyviä suunnitelmia, vaan ne olivat osana yritysten yleistä riskienhallintaa. Tämä on myös linjassa siinä, että aiempien kysymysten kohdalla osa vastaajista totesi, että tekoäly ei ole sinänsä sen kummempaa, kuin mikä tahansa muu uusi teknologia ja tästä syystä siihen käytetään pitkälti muiden teknologioiden yhteydessä käytettyjä metodeja. Vaikka riskienhallinta nousi vastauksissa vahvasti esille, haastateltavilta ei kuitenkaan kysytty tarkentavia lisätietoja riskienhallinnasta, sillä aihe ei ole tämän tutkimuksen keskiössä, vaikka se vastauksissa toistuukin. Vastausten pohjalta voidaan kuitenkin tehdä yleistys, että haastateltavien yrityksissä riskienhallinnalla on niin vahva osa tekoälyyn liittyen, että todennäköisesti Suomen finanssialalla käytetään tehokkaasti kirjallisuuskatsauksen luvun 3.1 kaltaisia menetelmiä liiketoiminnan riskejä arvioitaessa.

Kuten aiemmin todettiin, niin haastateltavien vastauksien pohjalta voidaan tehdä johtopäätös, että riskienhallinta on keskeisessä osassa liittyen tekoälyn haasteisiin ja riskeihin, sekä niiden tunnistamiseen. Jokainen haastateltava kuitenkin nimesi datan määrän ja keräyksen, sekä mahdolliset tietovuodot omasta mielestään suurimmiksi haasteiksi tai riskeiksi. Nämä kyseiset asiat tulisi kuitenkin ottaa huomioon yritysten riskienhallinnassa, joten tästä aiheesta voisi olla mahdollista pohtia sitä, että olisiko kuitenkin tarvetta erilliselle tekoälyä koskevalle riskienhallinnalle.

VA1: ” Ei ole varsinaisesti sellaista tekoälyspesifiä vahvasti. Finanssiala perustuu pitkälti luottamukseen ja se edellyttää riskienhallintaa, riskienhallintaa ja vielä vähän riskienhallintaa ja tekoäly on mukana siinä verkossa. Myös sääntely vaikuttaa paljon ”

FIVA: ” Riskiarviothan on sinänsä pakollisia ja me myös tarkastellaan näiden finanssialan yritysten sisäisten ohjeiden riittävyyttä ja tasoa. Onko niin kuin millaiset sisäiset ohjeet olemassa ja millä tasolla ne ovat. Kyllä minä sanoisin, että yleisesti Suomessa ollaan osaavia kuitenkin. Mutta kaikkiallahan näkyy resurssipula, ei vaan finanssialalla, vaan siis ihan ylipäätänsä it-teknologian, kyberosaajien, riskienhallinnan, yleinen osaajien pula. Hyvistä osaajista on tappelua ”

6 JOHTOPÄÄTÖKSET

Tässä luvussa käydään tarkemmin lävitse empiirisen tutkimuksen tuloksia, sekä pohditaan niiden merkittävyyttä. Luvussa vastataan tutkimuksen tutkimuskysymykseen, sekä apukysymykseen. Lisäksi arvioidaan tutkimuksen luotettavuutta ja pohditaan jatkotutkimusta. Empiirisen tutkimuksen avulla oli tarkoitus saada vastaus tutkimuskysymykseen: Millaisia tekoälyyn liittyviä haasteita tai riskejä Suomen finanssialalla koetaan ja varaudutaanko niihin? Edellisessä luvussa läpi käydyistä vastauksista on poimittu oleellisimmat haasteet ja riskit tiivistetysti taulukkoon, jotta saadaan vastauksista selkeämpi kuva (Taulukko 5).

Suomen finanssialan kokemat tekoälyyn liittyvät haasteet ja riskit liittyvät pääpiirteittäin tekoälyn tekemiin vääriin tulkintoihin ja päätöksiin, sekä hakkerointien ja muun rikollisuuden kehittymiseen. Lisäksi esille nousivat yleiset osaamiseen ja kouluttamiseen liittyvät haasteet, sekä suuriksi kasvavien datamäärien hallitseminen ja lisääntyvät tietovuodot. Taulukossa 5, kolme alinta saraketta, joissa X-merkintään on tehty lihavointi, ovat haastateltavien vastaamat, heidän omasta mielestään suurimmat haasteet ja riskit tekoälyyn liittyen.

TAULUKKO 5 Haastatteluissa todetut haasteet ja riskit.

Haaste/Riski	**PA1**	**PA2**	**VA1**	**FIVA**
Osaamiseen ja kouluttamiseen liittyvät haasteet.	X	X		X
Säännöksiin ja lakeihin liittyvät haasteet.				X
Blackboxeihin liittyvät riskit.				
Moraaliset ja eettiset haasteet.	X			X
Tekoälyn tekemät väärät tulkinnat ja päätökset.	X	X	X	X

(jatkuu)

Taulukko 5 (jatkuu)

Hakkerointien ja muun rikollisuuden kehittyminen.	X	X	X	X
Tekoäly muokkaa koko yhteiskuntaa.	**X**			
Valtaviksi kasvavat datamäärät ja lisääntyvät tietovuodot.		**X**	**X**	
Johdon tietoisuus, ymmärtäminen ja osaaminen.				**X**

6.1 Tulosten peilaaminen liiketoiminnan riskeihin

Tässä alaluvussa pohditaan, kuinka empiirisessä tutkimuksessa esille nousseet haasteet ja riskit sopivat yhteen kirjallisuuskatsauksen kohtaan 3.1, jossa käytiin lävitse riskiä yleisesti liiketoiminnan yhteydessä. Jokainen haastateltava nosti esille riskienhallinnan tärkeyden, joten vastauksia tulee tästä syystä peilata kyseiseen osioon kirjallisuuskatsauksesta. Suurimmiksi haasteiksi ja riskeiksi vastauksissa koettiin siis tekoälyn tekemät mahdolliset väärät tulkinnat, sekä hakkerointien ja muun rikollisuuden kehittyminen. Lisäksi vahvasti esiin nousi kouluttamiseen ja osaamiseen liittyvät haasteet, sekä valtavat datamäärät, jotka voivat johtaa lisääntyneisiin tietovuotoihin. Moraaliset ja eettiset haasteet mainittiin myös haastateltavien toimesta, mutta ne jätetään pois tulosten peilaamisessa kirjallisuuskatsaukseen. Perustelu pois jättämiselle on se, että vaikka moraaliset ja eettiset haasteet nousivat esille, niin jokainen ne haastatteluissa maininnut henkilö puhui niistä nimenomaan yleisesti tekoälyyn ja koko yhteiskuntaan liittyen, eikä finanssialaan liittyen.

Kirjallisuuskatsauksen alaluvussa 3.1 Riski liiketoiminnan yhteydessä, Drew (2007) jakoi yritysten kohtaamat riskit neljään luokkaan: taloudelliset, strategiset, toiminnalliset ja ulkoiset riskit. Empiirisen tutkimuksen tuloksissa suurimmiksi nousseet haasteet ja riskit jakautuvat näihin kaikkiin neljään luokkaan. Taloudellisiin riskeihin voidaan katsoa kuuluvaksi hakkeroinnit ja muu rikollisuus, sillä näillä voi olla suora taloudellinen vaikutus yritykseen. Strategisiin riskeihin lukeutuu osaamiseen ja kouluttamiseen liittyvät haasteet. Toiminnallisiin riskeihin voidaan katsoa kuuluvaksi valtaviksi kasvavat datamäärät ja tietovuodot, mutta myös hakkeroinnit ja muu rikollisuus voisi kuulua myös tämän kategorian alle, sillä yrityksen toiminnot tekevät hakkeroinnin mahdolliseksi, joko helposti tai vaikeasti. Tekoälyn tekemät väärät tulkinnat kuuluvat myös toiminnallisten riskien kategoriaan, mutta liitoksia voisi olla myös strategisiin riskeihin, sekä ulkoisiin riskeihin, mikäli väärät tulkinnat johtuvat ulkopuolisen tahon saastuttamasta datasta. Selkeimmin ulkoisten uhkien kategori-

aan kuuluu kuitenkin hakkeroinnit ja muu rikollisuus. Nämä uhat tulevat yleensä yrityksen ulkopuolelta, vaikka mukana voi olla myös yrityksen henkilökuntaa.

Kirjallisuuskatsauksessa esiteltiin Drewn ja Kendrickin (2005) tutkimuksen pohjalta kuviossa 4, yrityksille suunnattu malli riskiperusteisesta päätöksenteosta. Mallissa mahdollisen riskin todennäköisyyttä tulisi arvioida asteikolla matala/korkea, samalla asteikolla tulisi arvioida myös mahdollisen riskin seuraamuksia. Empiirisen tutkimuksen tuloksissa esille nousseet haasteet ja riskit peilattuna edellä mainittuun malliin sijoittuisivat kaikki samoihin kohtiin. Kuitenkin sillä erolla, että alakohtaisesti finanssialalla riskien toteutumisen todennäköisyys on melko korkea ja yksittäisen finanssialalla toimivan yrityksen kohdalla todennäköisyys ei ole aivan yhtä korkea. Finanssialalla toimii useita yrityksiä, kymmeniä tuhansia työntekijöitä, monia ohjelmistoja ja dataa kerätään useista lähteistä. Riski sille, että alalla yleisesti tulee tapahtumaan jokin haastatteluissa haasteeksi tai riskiksi koettu asia on korkea. Kuten todettu, ala on suuri ja siellä on paljon toimijoita, joten riskit toteutuvat väistämättä jollakin aikavälillä. Yksittäisen yrityksen kohdalla riskien toteutumisen todennäköisyyttä ei voida kutsua matalaksi, mutta se on matalampi kuin koko finanssialan todennäköisyys. Yrityksessä on vähemmän työntekijöitä, vähemmän ohjelmistoja ja erilaisia käytänteitä kuin koko alalla yhteensä, joten myös riskeihin valmistautuminen on mahdollista toteuttaa hyvin.

Mallin toinen osio koski mahdollisten riskien vaikutuksia skaalalla matala/korkea. Koko alaa ja yksittäistä finanssialalla toimivaa yritystä, koskee mahdolliset riskin toteutuman vaikutukset hieman eri tavalla. Yksittäisen yrityksen kohdalla vaikutukset olisivat tasolla korkea, sillä vaikutukset mainehaittojen lisäksi kohdistuisivat vain tähän yritykseen. Finanssialalla vaikutusten ei voida sanoa olevan matalat, mutta ne jäisivät kuitenkin koko alan kannalta huomattavasti pienemmiksi kuin yksittäisen yrityksen kohdalla. Todennäköisyyden ja vaikutuksen määrityksen jälkeen, Drewn ja Kendrickin (2005) malli antaa yrityksille toimintaohjeita, joiden avulla riskien kohtaaminen tulisi helpommaksi. Heidän mallinsa mukaiset toimintaohjeet olisivat aiemmin tehtyjen määritysten pohjalta Suomen finanssialalle ja alalla toimiville yrityksille seuraavanlaiset: kehitä asianmukainen valmius, rakenna tietoisuutta välttääksesi yllätykset ja kehitä yllättävien tapahtumien suunnitelma.

Haastateltavien joukossa ollut Finanssivalvonta, antoi vastauksissa sellaisen vaikutelman, että edellä mainittujen toimintaohjeiden mukaista toimintaa harjoitetaan finanssialalla valvojan taholla, niin Suomessa, kuin Euroopassa yhteistyötä tehden. Finanssialalla toimivien yritysten kohdalla toimintaohjeita varmasti noudatetaan myös entuudestaan pääasiassa hyvin, mutta tietoisuutta voi pyrkiä rakentamaan, sekä valmiutta ja suunnitelmia yllättävien tapahtumien varalle lisäämään yritysten sisällä. Riskien toteutuessa, vaikutukset ovat kuitenkin yksittäiselle yritykselle aina vakavammat kuin koko alalle.

6.2 Pohdinta

Tämän tutkimuksen kirjallisuuskatsauksessa vastattiin ensimmäiseen tutkimuskysymykseen: Millaisia tekoälyn yleistymiseen liittyviä haasteita tai riskejä finanssialan yritykset kokevat kansainvälisesti? Päällimmäisenä esiin nousivat työpaikkojen korvaantuminen tekoälyllä, yksityisyydensuojan rikkoutuminen, rikollisuuden kasvu ja kehittyminen, sekä sääntelylle tarvittavat uudet vaatimukset ja koneisiin liittyvät moraaliset ja eettiset haasteet. Tarkemmat vastaukset esitettiin kirjallisuuskatsauksen pohdinnan alaluvussa 3.3, koottuna taulukkoon 3. Empiirisen tutkimuksen osalta tavoite oli vastata tutkimuksen toiseen kysymykseen: Millaisia tekoälyyn liittyviä haasteita tai riskejä Suomen finanssialalla koetaan ja varaudutaanko niihin? Vastauksissa esiin nousivat tekoälyn tekemät väärät tulkinnat ja päätökset, hakkerointien ja muun rikollisuuden kehittyminen, osaamiseen ja kouluttamiseen liittyvät haasteet, sekä valtavaksi kasvavat datamäärät ja mahdolliset tietovuodot. Tämän tutkimuksen kolmas tutkimuskysymys oli: Millaisia eroja tai samankaltaisuuksia finanssialalla koetaan Suomessa ja kansainvälisesti, tekoälyn yleistymisen haasteisiin ja riskeihin liittyen? Tässä luvussa pohditaan vastausta viimeiseen tutkimuskysymykseen.

Kirjallisuuskatsauksessa todettiin maailmalla koettavan tekoälyn yleistymisen haasteena työpaikkojen korvaantuminen koneilla. Huangin ja Rustin (2018) mukaan analyyttista työtä vaativat korvaantuvat tekoälyllä. Javelosan (2017) mukaan korkeakoulutettu työ on vaarassa ja Russellin ym., (2015) mukaan matalapalkkainen työ korvaantuu tekoälyllä. Suomen finanssialalla tämä huoli ei noussut mitenkään erityisesti esille. Oikeastaan asia oli jopa päinvastoin, osa vastaajista totesi, että uskovat ammattitekijöitä aina olevan saatavilla ja osa koki, että osaajista on jopa pulaa. Toki vastauksissa nähtiin mielipiteitä tekoälyn koko yhteiskuntaa muokkaavasta voimasta ja sen voidaan nähdä liittyvän myös työpaikkojen muuttumiseen, mutta kokonaisuutena asiaa ei Suomessa koettu haasteena.

Kilpatrick (2018) ja Brundage (2018) kirjoittivat siitä, kuinka tekoälyn myötä riskit hakkeroinneille tulevat kasvamaan ja tietoturva haasteet lisääntyvät. Jin (2018) puolestaan kirjoitti yksityisyydensuojan rikkoutumisesta. Nämä kaikki koettiin riskeinä ja haasteina myös Suomen finanssialalla, sillä kaikki haastateltavat kertoivat kokevansa riskiksi hakkerointien ja muun rikollisuuden kasvamisen tekoälyn yleistymisen myötä. Hieman samaan kategoriaan menee Suomessa haasteeksi koettu datamäärien kasvu, ja siitä johtuvat mahdolliset tietovuodot ja niiden yleistyminen. Bostrom ja Yudkowsky (2011) kirjoittivat koneiden ihmismäisten moraalisten ja eettisten käsitteiden puuttumisesta. Myös suomessa nämä koettiin tekoälyyn liittyviksi haasteiksi.

Blackboxeihin liittyvistä haasteista kirjoittivat Adabi ja Berrada (2018), sekä Guidotti ym., (2019). Suomessa kyseisellä tekniikalla toteutettuja tekoälysovelluksia ei nähty ongelmallisina. Syy tähän oli yksinkertaisesti se, että Suomessa blackboxeja ei käytetä, sillä lait ja säännökset käytännössä estävät niiden käytön kokonaan. Gill (2016) kirjoitti tekoälyn tuovan uudenlaista tarvetta sääntelylle,

ja myös Suomessa Finanssivalvonta tunnisti tämän haasteen. He pohtivat ja tutkivat uusia säännöksiä yhdessä muiden Euroopan valvovien viranomaisten kanssa. Suomen finanssialalla nousi kaksi sellaista teemaa esille, joita ei kauheasti esiintynyt kansainvälisissä tutkimuksissa. Nämä olivat tekoälyn tekemät väärät tulkinnat ja osaamiseen ja kouluttamiseen liittyvät haasteet. Jokainen haastateltava kertoi kokemansa mahdolliset väärät tulkinnat ja päätökset riskeiksi. Osaamiseen liittyvät haasteet Suomessa kohdistuivat, niin yritysten johtoon, kuin työntekijöihin ja asiakkaisiin.

Pohdittaessa kansainvälisesti ja Suomessa koettujen haasteiden ja riskien erojen syitä, ensimmäisenä esiin tulee Suomen ja Euroopan yleensä tarkka sääntely. Tätä tukee myös viimeaikainen uutisointi siitä, miten Facebook, yksi maailman suurimmista yrityksistä uhkaa lopettaa toimintansa Euroopassa, sillä se kokee eurooppalaisen, käyttäjiä suojaavan tietosuojan olevan kiristystä heitä kohtaan (Kauppalehti, 2020.). Suomessa toiminta on avointa ja riskienhallinnalla on suuri rooli, ja se ennalta ehkäisee ongelmien syntymistä. Toinen huomioonotettava seikka on se, että kirjallisuuskatsauksen tutkimukset maailmalta ovat, jos eivät vanhoja, niin kuitenkin muutaman vuoden ikäisiä. Vaikka se ei ajallisesti ole kovin pitkä aika, niin tekoäly kehittyy kovaa vauhtia ja se voi tuoda omat eronsa ja vaikutuksensa jo muutamassa vuodessa. Esimerkkinä blackboxeihin liittyvät tutkimukset. Periaatteessa niitäkin olisi voinut olla enemmän käytössä, ainakin jollakin tasolla myös Suomessa ja Euroopassa ennen vuonna 2018 voimaan astunutta GDPR:ää.

Tekoälyyn ja sen yleistyvään käyttöön liittyy todella paljon samoja pääpiirteitä kuin digitalisoitumiseen ylipäätänsä. Tekoäly on valtavirtakäytössä kuitenkin vielä todella nuorta ja tilanteet voivat tulevaisuudessa muuttua. Tämä tutkimus kuitenkin puoltaa sitä, että nopeakaan muutos ei Suomen finanssialalla tule oleellisesti muuttamaan tai lisäämään haasteita tai riskejä. Sillä Suomessa haasteita ja riskejä mietitään ja otetaan huomioon niin säännöksiä laativan tahon puolesta, kuin tekoälysovelluksia käyttöönottavien yritysten puolella. Finanssialaa valvovan Finanssivalvonnan arvoihin on kirjoitettu ”ennakoimme toimintaympäristömme ja valvontakentän muutokset sekä kehitämme toimintaamme jatkuvasti” (Finanssivalvonta, 2018c). Tämän tutkimuksen pohjalta voidaan todeta kyseisen arvon myös näkyvän tekoälyyn liittyen Suomen finanssialalla. Tekoälyyn sovelletaan Suomessa myös samoja riskienhallintamenetelmiä, kuin mitä käytettäisiin minkä tahansa muun uuden teknologian tai asian yhteydessä.

6.3 Tutkimuksen luotettavuus

Kvantitatiivista, eli määrällistä tutkimusta mitataan yleensä reliabiliteetin ja validiteetin kautta. Laadullista tutkimusta ei voida arvioida kuitenkaan täysin samoin menetelmin kuin määrällistä (Saaranen-Kauppinen & Puusniekka, 2006). Tämän tutkimuksen empiirinen osuus toteutettiin laadullisena puolistrukturoituna haastattelututkimuksena ja kyseistä tutkimustyyppiä arvioi-

dessa, tulisi pohtia tutkimuksen uskottavuutta, luotettavuutta ja onko se toistettavissa.

Tutkimukseen osallistui neljä haastateltavaa henkilöä, mikä oli vähemmän kuin mitä alun perin oli suunniteltu. Pieni haastateltavien määrä vie hieman tutkimuksen uskottavuutta. Haastateltavat edustivat kuitenkin finanssialan sisällä eri osa-alueita, niin ammattinimikkeidensä kuin yritystensäkin puolesta. Haastateltavien ja haastattelijan äidinkieli oli sama, joten kielellisiltä ja kulttuurisilta väärinymmärryksiltä vältyttiin haastatteluiden toteuttamisen osalta. Osa haastateltavista on kuitenkin voinut ymmärtää eri tavalla joitakin käsiteltäviä asioita. Kysymykset olivat pääasiassa samassa järjestyksessä kaikilla haastateltavilla, mutta kyseisessä haastattelumenetelmässä oli tilaa myös lisäkysymyksille, joten haastattelut eivät olleet täysin identtisiä keskenään. Haastatteluita ei voitu järjestää kasvokkain, johtuen vallitsevasta Covid-19 pandemiasta. Kaikki haastattelut toteutuivat kuitenkin videoyhteyden välityksellä. Tämän tutkimuksen tuloksia olisi lähes mahdoton saada täysimääräisesti toistettua uudella tutkimuksella, sillä se vaatisi samat haastateltavat, samojen keskusteluiden ja kysymysten kanssa. Toistettavuus tai sen haasteellisuus, ei kuitenkaan ole tämän kaltaisen tutkimuksen päätavoite. Tutkimus tuotti tuloksissaan vertailua eroavaisuuksien ja samankaltaisuuksien välillä ja ajan kuluessa nämä erot ja yhtäläisyydet tulevat muuttumaan, joko lähemmäksi tai kauemmaksi toisistaan. Mikäli tutkimus toteutettaisiin ajallisesti hyvin nopeasti tämän tutkimuksen jälkeen, niin tulokset olisivat mahdollisesti hyvin saman suuntaisia kuin tässä tutkimuksessa. Tekoäly ja finanssiala muuttuvat kuitenkin hyvin nopeasti ja tutkimustulosten toistettavuus vähenee ajan kuluessa entisestään.

Tutkimus ja tutkimuksessa pohjana käytetyt haastattelukysymykset olivat siinä mielessä onnistuneet, että niiden pohjalta saatiin vastattua kaikkiin tutkimuksen tavoitteisiin, eli tutkimuskysymyksiin. Tutkimuksessa on erittäin pieni todennäköisyys sille, että tutkijan omat mielipiteet tai ennakkoasenteet olisivat vaikuttaneet tutkimustuloksiin, sillä tutkimuksessa verrattiin kirjallisuuskatsauksen ja empiirisen tutkimuksen samankaltaisuuksia ja eroavaisuuksia. Tämän kaltaisessa vertailussa mielipiteet ja asenteet eivät yleensä tule suuresti vaikuttaen esille.

6.4 Jatkotutkimus

Tutkimuksen tekovaiheessa heräsi useita aiheita mahdollisille jatkotutkimuksille. Tämän tutkimuksen empiirisessä osiossa tutkittiin, millaisia erilaisia haasteita tai riskejä finanssialalta löytyy tekoälyn yleistymiseen liittyen. Jatkotutkimuksessa voisi keskittyä tutkimaan tarkemmin jotakin haasteeksi tai riskiksi koettua osa-aluetta. Tällainen osa-alue voisi olla esimerkiksi tekoälyyn liittyvät suuret datamäärät, jotka koettiin haasteellisiksi tämän tutkimuksen yhteydessä. Lisääntyvät tietovuodot suurien datamäärien yhteydessä aiheuttivat myös huolia, joten yksi mahdollinen jatkotutkimus aihe voisikin olla, datan huolellinen, eettinen tai yhdenvertainen käyttö tekoälyn yhteydessä. Toinen vaihtoehto olisi

tutkia tarvetta tekoälyspesifioidulle riskienhallinnalle, sillä tämän tutkimuksen yhteydessä kävi ilmi, että tekoälyyn suhtaudutaan kuin mihin tahansa muuhunkin uuteen teknologiaan, mutta samalla suurimmat haasteet ja riskit koettiin riskienhallinnan alle liittyviin tietojen keräämiseen ja tietovuotoihin.

Tässä tutkimuksessa nousi esille haasteena myös tekoälyyn liittyvä osaaminen ja kouluttaminen. Lisäksi yksi haastateltavista nosti esille, että vaikka chattibotit hyödyttävät niin asiakasta kuin työntekijää, niin siitä huolimatta suuri osa asiakkaista ei pidä lainkaan chattibottien käyttämisestä, ja osa suorastaan vihaa niitä. Tästä voisi saada mahdollisen jatkotutkimusaiheen, eli yhdistämällä hieman näitä kahta esitettyä asiaa, voitaisiin tutkia minkä takia chattibotteja, muuta tekoälyä tai uutta teknologiaa vihataan tai siitä ei tykätä. Johtuuko se juuri osaamisen puutteesta vai onko käytettävyys jollakin tavoin sekavaa tai vaikeaa, vai onko taustalla vain se, että ei haluta omaksua uutta teknologiaa sillä vanha tapa toimia koetaan riittävän hyväksi. Tästä tutkimuksesta poiketen, jatkotutkimuksessa voitaisiin yritysten sijasta keskittyä finanssialan asiakkaisiin ja tutkia heidän, tekoälyyn liittyviä kokemuksiaan. Samoin tutkimusmenetelmänä voisi tämän kaltaisessa jatkotutkimuksessa toimia määrällinen tutkimus laadullisen sijasta. Tutkimuksen ei myöskään olisi välttämättä rajoituttava ainoastaan Suomen finanssialan yritysten asiakkaisiin. Määrällinen tutkimus kyselylomakkeella toteutettuna olisi myös mahdollista toteuttaa laadullista helpommin laajemmalla alueella, esimerkiksi pohjoismaissa tai Euroopassa.

Tämän tutkimuksen pohjalta voidaan sanoa, että Suomen finanssialalla ollaan hyvin perillä tekoälyyn liittyvistä haasteista ja riskeistä. Päällimmäisinä syinä voidaan todeta laadukas ja ajantasainen säännösten ja valvonnan olemassaolo, sekä yritysten harjoittamat riskienhallintatoimet. Näihin asioihin voisi olla mahdollista paneutua tarkemmin. Finanssivalvonnalta tai finanssialan yritykseltä voisi kysyä säännöksiin tai riskienhallintaan liittyvää, tekoälyyn yhdistettyä aihetta tai jopa case-tapaustutkimusta aiheeseen liittyen. Yksi mahdollinen aihe tapaustutkimukselle voisi olla tutkia koko käyttöönottoprosessia, kun otetaan käyttöön jotain kokonaan uutta tekoälyohjelmistoa. Tähän voisi ottaa haastatteluihin henkilöitä ohjelmiston käyttöönottavasta yrityksestä ja myös ohjelmiston toimittavasta yrityksestä. Tekoäly kehittyy jatkuvasti ja finanssiala on myös melko nopeasti uutta teknologiaa omaksuva ala, joten kaikkia sopivia aiheeseen liittyviä jatkotutkimusaiheita on vaikea tai lähes mahdotonta rajata tässä vaiheessa.

7 YHTEENVETO

Tässä pro gradu tutkielmassa oli tarkoituksena selvittää millaisia haasteita ja riskejä Suomen finanssialalla tunnistetaan ja koetaan yleistyvän tekoälyn käytön yhteydessä. Varsinaisia tutkimuskysymyksiä oli kolme. Ensimmäinen tutkimuskysymys oli: millaisia tekoälyn yleistymiseen liittyviä haasteita tai riskejä finanssialan yritykset kokevat kansainvälisesti? Vastausta tähän kysymykseen lähdettiin selvittämään aiempien tutkimusten kautta kirjallisuuskatsauksen muodossa. Aiempaa tutkimusta aiheesta oli riittävästi, ja sen avulla saatiin muodostettua selkeä kuva siitä millaisia haasteita ja riskejä maailmalla koetaan. Tekoälyn koettiin korvaavan niin korkeasti koulutettua työtä, kuin matalapalkkaista työtä, sekä analyyttisia taitoja vaativia töitä. Lisäksi kirjallisuuskatsauksen perusteella todettiin, että riskit hakkeroinneille ja muulle rikollisuudelle lisääntyvät tekoälyn myötä. Myös tietoturvaongelmien koettiin kasvavan ja yksityisyydensuojan rikkoutuvan, ja johtaen jopa yksityishenkilöiden kiristyksiin. Esille nousi myös tarve uudenlaiselle sääntelylle ja valvonnalle, sekä kaiken tekoälyn tarvitsevan aineistoin muuttaminen digitaaliseen muotoon. Moraaliset ja eettiset käsitykset koettiin myös haasteellisiksi, sillä tekoälyä käyttävät koneet eivät näitä ihmismäisiä piirteitä omaa. Niin kutsutun blackbox-tekniikan riskeistä kirjoitti myös useampi tutkija, kuten myös supertekoälyyn liittyvistä vaaroista.

Tutkimuksen toinen tutkimuskysymys oli: Millaisia tekoälyyn liittyviä haasteita tai riskejä Suomen finanssialalla koetaan ja varaudutaanko niihin? Tähän tutkimuskysymykseen lähdettiin vastausta hakemaan laadullisen empiirisen tutkimuksen kautta, puolistrukturoitujen haastatteluiden avulla. Lopulliseen tutkimukseen saatiin neljän finanssialan yrityksissä työskentelevän henkilön haastattelua. Haastateltavat edustivat Finanssivalvontaa, vakuutusyhtiön varainhoito-osastoa ja kahta eri pankkia. Sen lisäksi, että kaikki haastateltavat työskentelivät finanssialalla, heidän työnkuvaansa liittyi myös tekoälyn kanssa työskentely. Kaikille haastateltaville toimitettiin ennakkoon kysymykset, jotta he pystyivät valmistautumaan haastatteluihin. Kaikki haastattelut toteutettiin videoyhteyden avulla huhtikuun ja kesäkuun 2020 välisenä aikana. Haastatteluiden perusteella löytyi kaksi sellaista haastetta tai riskiä, jotka tulivat nimetyksi jokaisen haastateltavan puolesta. Nämä olivat hakkerointien ja muun ri-

kollisuuden lisääntyminen, sekä tekoälyn tekemät väärät tulkinnat ja päätökset. Lisäksi suurin osa vastaajista nimesi tekoälyyn liittyvän osaamisen ja kouluttamisen olevan haasteiden joukossa. Mainitsemisen arvoisiksi haasteiksi koettiin myös valtaviksi kasvavat datamäärät, jotka saattavat lisätä tietovuotojen määriä. Lisäksi esille nousi säännöksiin ja lakeihin liittyvät haasteet, sekä moraaliset ja eettiset tekoälyyn liittyvät haasteet.

Kolmannen tutkimuskysymyksen avulla pyrittiin löytämään samankaltaisuudet ja eroavaisuudet Suomen ja kansainvälisen finanssialan tekoälyyn liittyvien haasteiden ja riskien välillä, eli vertailtiin kahden ensimmäisen tutkimuskysymyksen tuloksia toisiinsa. Merkittävin eroavuus liittyi työpaikkojen menettämiseen. Siinä missä kansainvälisesti koettiin riskiksi se, että tekoäly korvaa työpaikkoja, niin Suomessa asiaa ei nähty riskinä. Osa haastateltavista koki, että osaavista työntekijöistä on ajoittain jopa pula ja osa taas vastasi, että osaavia tekijöitä löytyy aina. Toinen suuri merkittävä eroavuus liittyi blackbox-tekniikkaa hyödyntäviin tekoälysovelluksiin. Suomessa tämän tyyppisiä ohjelmistoja ei koettu haasteellisiksi, sillä Suomessa ja Euroopassa lainsäädäntö käytännössä estää kyseisten ohjelmistojen käytön kokonaan. Merkittävimmät yhtäläisyydet löytyivät uskosta hakkerointien ja muun rikollisuuden kasvamisesta, sekä yksityisyydensuojan rikkoutumisen lisääntymisestä tekoälyn yleistyvän käytön vuoksi. Muita yhtäläisyyksiä löytyi liittyen eettisiin ja moraalisiin haasteisiin, sekä säännösten ja valvonnan mukautumiseen. Vertailun lopussa empiirisen tutkimuksen päätuloksia peilattiin kirjallisuuskatsauksen liiketoiminnan riskien malleihin.

Tutkimuksen loppuosiossa pohdittiin tutkimuksen luotettavuutta. Kritiikki kohdistui haastateltavien suhteellisen pieneen lukumäärään ja tutkimuksen toistettavuuteen. Täsmälleen samanlaisiin tuloksiin olisi lähes mahdotonta päästä uusimalla tutkimus, sillä se vaatisi identtiset olosuhteet. Tämän tyylisessä vertailevassa tutkimuksessa tulosten täsmällinen toistettavuus ei tosin ole tutkimuksen päätavoite. Tekoäly, finanssiala ja näiden keskinäiset yhteydet työntekijöineen ja uusine ohjelmistoineen muuttuvat nopeaa vauhtia, joten uusitun tutkimuksen tulokset olisivat varmasti erilaisia. Tutkimus koettiin onnistuneeksi, sillä haastateltavat olivat ammattinsa ja kokemuksensa puolesta sopivia vastaamaan haastatteluihin. Tutkimuksen avulla onnistuttiin myös vastaamaan tutkimuskysymyksiin. Lopuksi pohdittiin erilaisia jatkotutkimus aiheita, joista päällimmäisenä nousi esiin tekoälyn osaamiseen liittyvät haasteet finanssialan asiakkaan näkökulmasta.

LÄHTEET

Adadi, A., Berrada, M. (2018). Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI). *IEEE Access*, vol. 6, pp. 52138-52160, 2018.

Artis, M., Ayuso, M., Guillén, M. (2002). *Detection of automobile insurance fraud with discrete choice models and misclassified claims.* The Journal of Risk and Insurance. Volume69, Issue 3. pp. 325-340.

Azulay, D. (2019). *Artificial Intelligence in Finance – a Comprehensive Overview.* Emerj. December, 2019.

BlackRock. (2020). *Aladdin FAQs.* Haettu 27.08.2020 osoitteesta https://www.blackrock.com/aladdin/resources/faqs

Boston Consulting Group, (2019). *Global Wealth 2019. Reigniting Radical Growth.* Haettu 15.08.2020 osoitteesta https://image-src.bcg.com/Images/BCG-Reigniting-Radical-Growth-June-2019_tcm9-222638.pdf

Bostrom, N., Yudkowsky, E. (2011). The Ethics of Arttificial Intelligence. *Cambridge Handbook of Artificial Intelligence.* Cambridge University Press, 2011.

Brookshear, J. G. (1989). *Theory of Computation: Formal Languages, Automata, and Complexity.* Redwood City, California: Benjamin/Cummings Publish Company, Inc.

Brougham, D. & Haar, J. (2018). *Smart Technology, Artificial Intelligence, Robotics, and Algorithms (STARA): Employees' perceptions of our future workplac.* Journal of Management and Organization. Lyndfield Vol. 24, Iss. 2, March 2018.

Brundage, M., Avin, S., Clark, J. (2018). *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*. Future of Humanity Institute, University of Oxford. 2018

Cambridge Dictionary. (2020). "*Challenge definition*". Haettu 24.06.2020 osoitteesta dictionary.cambridge.org/dictionary/english/challenge.

Caron, L., Dionne, G. (1999). *Insurance Fraud Estimation: More Evidence From the Quebec Automobile Insurance Industry in:* G. Dionne and C. Laberge-Nadeau. Automobile Insurance: Road Safety, New Drivers, Risks, Insurance Fraud and Regulation. *Springer, Boston, MA.*

Cormen, T.H., Leiserson, C.E., Rivest, R.L., Stein, C. (2009). *Introduction to Algorithms, Third Edition.* The MIT Press, Cambridge, Massachusetts. ISBN 978-0-262-53305-8.

DailyMail, (2015). *Two suicides are linked to Ashley Madison leak: Texas police chief takes his own life just days after his email is leaked in cheating website hack*. Haettu 28.08.2020 osoitteesta https://www.dailymail.co.uk/news/article-3208907/The-Ashley-Madison-suicide-Texas-police-chief-takes-life-just-days-email-leaked-cheating-website-hack.html

Drew, M. (2007). *Information risk management and compliance – expect the unexpected*. BT Technology Journal 25, 19–29. January 2007.

Drew, S. A. & Kendrick, T. (2005). *Risk Management: The Five Pillars of Corporate Governance*. Journal of General Management. Volume 31, Issue 2, pp. 19-36, 2005.

Drew, S. A., Kelley, P. C. & Kendrick, T. (2006). *CLASS: Five elements of corporate governance to manage strategic risk*. Business Horizons, Vol 49, Issue 2, 2006. pp. 127-138. ISSN 0007-681.

Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen.* Tampere: Vastapaino.

Euroopan keskuspankki. (2020). *Tehtävät.* Haettu 27.07.2020 osoitteesta https://www.ecb.europa.eu/ecb/tasks/html/index.fi.html

Finanssiala, (2019). *Veropäivä 2019.* Haettu 14.07.2020 osoitteesta https://www.finanssiala.fi/uutismajakka/Sivut/Veropaiva-2019.aspx

Finanssivalvonta, (2018a). *Toimivalta ja toiminnan rahoitus.* Haettu 07.08.2020 osoitteesta https://www.finanssivalvonta.fi/finanssivalvonta/toimivalta-ja-rahoitus/

Finanssivalvonta, (2018b). *Hallinnolliset seuraamukset*. Haettu 10.08.2020 osoitteesta https://www.finanssivalvonta.fi/finanssivalvonta/toimivalta-ja-rahoitus/toimivalta/hallinnolliset-seuraamukset/

Finanssivalvonta, (2018c). *Arvot ja strategia.* Haettu 04.10.2020 osoitteesta https://www.finanssivalvonta.fi/finanssivalvonta/arvot-ja-strategia/

Finanssivalvonta, (2020a). *Tietoa Finanssivalvonnasta*. Haettu 01.07.2020 osoitteesta https://www.finanssivalvonta.fi/finanssivalvonta/

Finanssivalvonta, (2020b). *FinTech – Finanssialan innovaatiot*. Haettu 02.07.2020 osoitteesta https://www.finanssivalvonta.fi/pankki/fintech-finanssialan-innovaatiot/

Finanssivalvonta, (2020c). *Tietoa Finanssivalvonnasta.* Haettu 04.08.2020 osoitteesta https://www.finanssivalvonta.fi/finanssivalvonta/

Finanssivalvonta, (2020d). *Valvottavien ja muiden maksuvelvollisten lukumäärä.* Haettu 29.06.2020 osoitteesta https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/toimintakertomukset/toimintakertomus-2019/finanssivalvonta/liitteet/valvottavien-ja-muiden-maksuvelvollisten-lukumaara/

Finanssivalvonta, (2020e). *Varautuminen.* Haettu 17.08.2020 osoitteesta https://www.finanssivalvonta.fi/saantely/varautuminen/

Finlex, (2008). *Laki Finanssivalvonnasta 878/2008*.Haettu 07.08.2020 osoitteesta https://www.finlex.fi/fi/laki/ajantasa/2008/20080878

Gardner, H. (1999). Intelligence reframed: *Multiple intelligences for the 21st century*. Basic Books.

Gartner. (2018). *Gartner Survey Shows 27 Percent of Finance Departments Expect to Deploy Artificial Intelligence by 2020*. Haettu 12.06.2020 osoitteesta https://gartner.com/en/newsroom/pressreleases/2018-12-06-gartner-survey-shows-27-percent-of-financedepartments-expect-to-deploy-artificial-intelligence-by-2020.

Geist, E.M. (2015). *Is artificial intelligence really an existential threat to humanity*? Bulletin of the Atomic Scientists.

Gill, K.S. (2016). Artificial super intelligence: beyond rhetoric. *AI & Society,* May 2016, Volume 31, Issue 2, pp 137–143.

Glancy, F. H., & Yadav, S. B. (2011). *A computational model for financial reporting fraud detection*. Decision Support Systems, 50(3), 595-601.

Guidotti, R., Monreale, A., Pedreschi, D. (2019). *The AI Black Box Explanation Problem*. ERCIM News. Special theme: Transparency in Algorithmic Decision Making. Number 116, January, 2019.

Hirsjärvi, S., Remes, P., & Sajavaara, P. (2000). *Tutki ja kirjoita*. 5. painos. Helsinki: Tammi.

Hockstein, N. G., Gourin, C. G. & Faust, R. A. (2007). *A history of robots: from science fiction to surgical robotics.* Springer London 2007.

Huang, M-H & Rust, R. (2018). *Artificial Intelligence in Service*. Journal of Service Research. Volume 21, issue 2, page(s): 155-172.

Javelosa, J. (2017). Major Firm Announces It's Replacing Its Employees with A.I. *Futurism.* April, 2017.

J.P. Morgan (2020). *Demystifying New Technologies in Treasury*. Haettu 02.09.2020 osoitteesta https://www.jpmorgan.com/solutions/treasury-payments/insights/demystifying-tech.

Kaplan, A. & Haenlein, M. (2019). *Siri, Siri in my Hand, who's the Fairest in the Land?* On the Interpretations Illustrations and Implications of Artificial Intelligence. Business Horizons, 62(1), 15-25.

Kauppalehti (2020). *Facebook vihjaa lähtevänsä Euroopasta – Taustalla Irlannin tietosuojaviranomaisen päätös.* Haettu 07.10.2020 osoitteesta https://www.kauppalehti.fi/uutiset/facebook-suuttui-uhkaa-lahtea-euroopasta-taustalla-irlannin-tietosuojaviranomaisen-paatos/07283aa4-3adf-4420-bdb2-582d15cf09e9

Khandani, A. E., Kim, A. J., & Lo, A. W. (2010). Consumer credit-risk models via machine-learning algorithms. *Journal of Banking & Finance, 34(11),* 2767–2787.

Kilpatrick, H. (2018). *The Threats Artificial Intelligence Poses to Cybersecurity*. ScienceSoft, Professional Software Development. Sep, 5. 2018.

Kostka, G. (2019). *China's social credit systems and public opinion: Explaining high levels of approval.* New Media & Society, Vol 21, Issue 7, 2019.

Kuusela, H. & Ollikainen, R. (2005). Riskit ja riskienhallinta. Tampereen Yliopistopaino Oy – Juvenes Print.

Lamberton, C., Brigo, D. & Hoy, D. (2017). *Impact of Robotics, RPA and AI on the Insurance Industry: Challenges and Opportunities*. Journal of Financial Perspectives, Vol. 4, No. 1, May 2017

Lapatto, M. (2019). *Finanssialalla 3,2 miljardin euron verojalanjälki*. Finanssiala RY.

Mansingh, G. (2015). *Profiling internet banking users: A knowledge discovery in data mining process model based approach*. Information Systems Frontiers, 17(1), 193-215.

McCarthy, J., & Hayes, P. J. (1969). Some philosophical problems from the standpoint of artificial intelligence. *Computer Science Department, Stanford University.*

McCarthy, J. (2007). *What is Artificial Intelligence?* Stanford University. Haettu 06.07.2020 osoitteesta http://www-formal.stanford.edu/jmc/whatisai.pdf

Mehrotra, A. (2019). *Artificial Intelligence in Financial Services – Need to Blend Automation with Human Touch*. 2019 International Conference on Automation, Computational and Technology Management (ICACTM). London, United Kingdom, 2019, pp. 342-347.

Myers, M. D. & Newman, M. (2007). *The qualitative interview in IS research: Examining the craft*. Information and organization, pp. 2-26, volume 17, issue 1, 2007.

Patterson, J. & Gibson, A. (2017). *Deep Learning: A Practitioner's Approach* (1st. ed.). O'Reilly Media, Inc.

Peng, Y., Kou, G., Sabatka, A., Chen, Z., Khazanchi, D., Shi, Y. (2006). *Application of Clustering Methods to Health Insurance Fraud Detection*. 2006 International Conference on Service Systems and Service Management. Troyes, 2006, pp. 116-120.

RBC, (2019). *RBC's MyAdvisor delivers digital experience with a human touch: 1 million Canadians now connected with digital plan and live advisors.* Haettu 16.09.2020 osoitteesta http://www.rbc.com/newsroom/news/2019/20190528-myadvisor.html

Rubin, H.J., & Rubin, I.S. (2005). *Qualitative interviewing: the art of hearing data*. 2nd Edition. Thousand Oaks; London; New Delhi: Sage Publications, 2005.

Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *Tutkimuksen luotettavuus ja arviointi*. KvaliMOTV- Menetelmäopetuksen tietovaranto. Tampere: Yhteiskuntatieteellinen tietoarkisto.

Saidam, D. (2019). *Mastercard-launches-threat-scan-to-assess-bank-fraud-exposure*. Mastercard. Haettu 24.08.2020 osoitteesta https://mastercardcontentexchange.com/newsroom/press-releases/2019/october/mastercard-launches-threat-scan-to-assess-bank-fraud-exposure/

Shalev-Shwartz, S. & Ben-David, S. (2014). *Understanding Machine Learning:FromTheory to Algorithms.* Cambridge University Press, 2014.

Shang, K. (2018). *Applying Image Recognition to Insurance.* Society of Actuaries.

Siukonen, T. & Neittaanmäki, P. (2019). *Mitä tulisi tietää tekoälystä*. Docendo.

Stanford Encyclopedia of Philosphy. (2017) "*Risk definition* ". Haettu 24.06.2020 osoitteesta https://plato.stanford.edu/entries/risk/

Suomen Pankki. (2020a). *Historia.* Haettu 27.07.2020 osoitteesta https://www.suomenpankki.fi/fi/suomen-pankki/historia2/

Suomen Pankki. (2020b). *Tehtävät.* Haettu 27.07.2020 osoitteesta https://www.suomenpankki.fi/fi/suomen-pankki/tehtavat/

Swamy, K., Pashley, M., & Gilbert, E. (1997). *Neural Network Applications in Finance*. Conference: Fourth Annual Meeting of The American Society of Business and Behavioral Sciences, February 1997.

Tao, H., Zhixin, L., Xiaodong, S. (2012). *Insurance fraud identification research based on fuzzy support vector machine with dual membership. 2012* International Conference on Information Management, Innovation Management and Industrial Engineering, Sanya, 2012, pp. 457-460.

Tieto, (2018). *Tekoäly suorittaa, ihminen johtaa.* Haettu 19.8.2020 osoitteesta https://www.tieto.com/fi/uutishuone/kaikki-uutiset-ja-tiedotteet/blogit/2018/tekoaly-suorittaa-ihminen-johtaa/

Trippi, R. & Turban, E. (1992). *Neural Networks in Finance and Investing:* Using Artificial Intelligence to Improve Real World Performance. McGraw-Hill, Inc., USA.

Turchin, A., Denkenberger, D. (2018). *Classification of global catastrophic risks connected with artificial intelligence.* AI & Society. Springer London. 2018.

Turing, A. (1950). Computing Machinery and Intelligence. *Mind, 59(236), 433–460.*

LIITE 1 HAASTATTELUKYSYMYKSET

Haastateltavan taustatiedot:

1. Kerro hieman itsestäsi, eli kuka olet ja mitä teet työksesi?

2. Kuinka kauan olet työskennellyt nykyisessä tehtävässä?

3. Kuinka kauan olet työskennellyt finanssialalla?

Tekoälyn rooli yrityksessä:

4. Onko teidän yrityksessänne tekoälyä käytössä? Millä eri liiketoiminnan osa-alueilla?

5. Onko teidän yrityksessänne osa-alueita, joissa on ollut käytössä tekoälyä, mutta sen käytöstä on myöhemmin luovuttu? Miksi siitä on luovuttu?

6. Onko teidän yrityksessänne suunnitelmissa ottaa lähitulevaisuudessa tekoälyä käyttöön osa-alueilla, joissa sitä ei aiemmin ole käytetty?

7. Onko tekoälyn käytöstä ollut konkreettista hyötyä yrityksessänne? Millaista hyötyä ja millä osa-alueilla?

Tekoälyyn liittyvät haasteet ja riskit:

8. Millaisin keinoin yrityksessänne pyritään tunnistamaan tekoälyn yleistymiseen liittyviä mahdollisia haasteita tai riskejä?

9. Koetteko tekoälyn tuovan riskejä tai haasteita henkilöstöön liittyen (esimerkiksi rekrytointien tai koulutusten yhteydessä, kun uudenlainen teknologia vaatii uudenlaista osaamista)?

10. Koetteko lakien tai säännösten tuovan haasteita tai riskejä tekoälyn yleistymiseen liittyen? Miten otatte nämä huomioon (esimerkiksi GDPR)?

11. Koetteko haasteita tai riskejä Blackbox-tekniikalla toteutettuihin

tekoälyohjelmistoihin liittyen? (Blackbox on ”laatikko”, jonka sisällä algoritmi tekee päätökset, mutta päätökseen johtavat syyt ja johtopäätökset eivät ole saatavilla).

12. Koetteko tekoälyn lisääntyvään käyttöön liittyvän moraalisia tai eettisiä haasteita?

13. Useat finanssialan tarjoamat palvelut mielletään henkilökohtaista kanssakäymistä vaativiksi palveluiksi. Koetteko tekoälyn muokkaavan palveluita entistä kasvottomampaan suuntaan vai tekevän palveluista entistä henkilökohtaisempaa?

14. Koetteko tekoälyn mahdollisten virheellisten tulkintojen tuovan haasteita tai riskejä tekoälyn käyttöön liittyen? Millaisia?

15. Tekoälyn yleistyminen voi tuoda mukanaan uudenlaisia kohdennettuja hyökkäyksiä tai muunlaista uutta entistä edistyneempää rikollisuutta. Miten nämä seikat tulisi ottaa huomioon tekoälyn käytössä tai käyttöönoton suunnittelussa?

16. Kuinka näette tekoälyn tekemien päätösten lopullisen vastuun jakautuvan? Onko jokainen tapaus erilainen vai onko vastuussa aina esimerkiksi tekoälyä käyttävä yritys tai tekoälyn kehittänyt yritys?

17. Mitkä asiat koet suurimmiksi haasteiksi tai riskeiksi tekoälyn yleistyvään käyttöön liittyen?

18. Onko tunnistettuihin riskeihin tai haasteisiin varauduttu tai niitä varten tehty suunnitelmia? Millaisia?

19. Onko sinulla muita huomioita aiheeseen liittyen, joita haluaisit tuoda esiin?