

Olli Pesari

KONEOPPIMINEN TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA

Johtamisen ja talouden tiedekunta

Kandidaatintutkielma

Joulukuu 2025

Ohjaaja: Akseli Kettula

TIIVISTELMÄ

Olli Pesari: Koneoppiminen terveystakuutuspetosten tunnistamisessa

Kandidaatintutkielma

Tampereen yliopisto

Kauppatieteiden tutkinto-ohjelma

Joulukuu 2025

Vakuutuspetokset ovat merkittävä ongelma vakuutusosalalla niiden aiheuttaessa suoria taloudellisia menetyksiä ja heikentäessä vakuutusjärjestelmän luotettavuutta. Petosten havaitsemista vaikeuttaa se, että vilpallinen toiminta sulautuu usein osaksi normaaleja hoito- ja korvausprosesseja, jolloin yksittäiset petostapaukset jäävät helposti piiloon manuaalisen valvonnan ja sääntöpohjaisten järjestelmien ulottumattomiin. Manuaalinen valvonta puolestaan on usein sekä hidasta että rajoitteista. Teknologinen kehitys ja koneoppimismenetelmät, tarjoavat uusia mahdollisuuksia ongelman ratkaisemiseen.

Tämän tutkielman tavoitteena on selvittää, miten koneoppimismenetelmiä voidaan hyödyntää terveystakuutuspetosten tunnistamisessa ja ehkäisemisessä, sekä millaista tietoa nämä menetelmät käyttävät petoksen havaitsemisen perusteena. Näihin kysymyksiin vastataan kahden tutkimuskysymyksen avulla: 1. Miten koneoppimismenetelmiä hyödynnetään terveystakuutuspetosten tunnistamisessa? ja 2. Millaisia tietoja ja muuttujia petosten havaitsemisessa käytetyt menetelmät hyödyntävät?

Tutkimus toteutettiin systemaattisena kirjallisuuskatsauksena, ja aineisto analysoitiin aineistolähtöisen sisällönanalyysin avulla. Tulosten perusteella koneoppimismenetelmät hyödyntävät laajaa tietopohjaa, joka ulottuu laskutuksen ja hoitotoimenpiteiden määristä palveluntarjoajan profiileihin ja hoitoketjujen johdonmukaisuuteen. Yksittäiset muuttujat eivät ole ratkaisevia, vaan petollinen toiminta paljastuu usein epätavallisista yhdistelmistä ja toiminnan rakenteellisista muutoksista. Koneoppimismenetelmistä erityisesti puupohjaiset mallit sekä valvottujen ja valvomattomien menetelmien yhdistelmät, eli ”hybridimallit” osoittautuivat tehokkaiksi. Menetelmien onnistunut käyttö edellyttää kuitenkin laadukasta ja suurta datamäärää, epätasapainoisen aineiston asianmukaista käsittelyä sekä mallien tulkittavuutta, jotta saatuja tuloksia voidaan hyödyntää käytännössä.

Yhteenvetona tutkimus osoittaa, että koneoppiminen tarjoaa lupaavan välineen terveystakuutuspetosten havaitsemiseen. Sen avulla valvontaa voidaan kohdentaa aiempaa tarkemmin ja ennakoivammin, kunhan käytettävä data on riittävän kattavaa ja menetelmät läpinäkyviä.

Avainsanat: koneoppiminen, terveystakuutuspetokset, vakuutusala, riskienhallinta

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

TEKOÄLYN KÄYTTÖ OPINNÄYTTEESSÄ

Opinnäytteessäni on käytetty tekoälysovelluksia:

- Ei
- Kyllä

Ilmoitukseni mukaan olen käyttänyt opinnäytteessäni tutkielmaprosessin aikana seuraavia tekoälysovelluksia:

Tekoälysovellusten nimet ja versiot:

ChatGPT 5o

Copilot

Scopus AI

Käyttötarkoitus: Tässä tutkielmassa tekoälyä hyödynnettiin työkaluna kirjoitusprosessin aikana. Tekoälyä käytettiin esimerkiksi ideoiden jäsentämiseen, hakusanojen ja lähteiden etsintään sekä kielen selkeyttämiseen. Lisäksi sitä hyödynnettiin tekstin muotoilun ja sanavalintojen tarkentamisessa sekä englanninkielisen aineiston kääntämisessä ja tiivistämisessä.

Osiot, joissa tekoälyä on käytetty: Tekoälyä on hyödynnetty tutkielman kaikissa osioissa kielenhuollon tukena sekä englanninkielisen aineiston kääntämisessä ja tiivistämisessä. Sen tehtävänä on ollut esimerkiksi selkeyttää ilmaisuja ja yhtenäistää kirjoitustyyliä.

Olen tietoinen siitä, että olen täysin vastuussa koko opinnäytteeni sisällöstä, mukaan lukien osat, joissa on hyödynnetty tekoälyä, ja hyväksyn vastuun mahdollisista eettisten ohjeiden rikkomuksista.

SISÄLLYSLUETTELO

KUVIO- JA TAULUKKOLUETTELO	6
1 JOHDANTO	7
1.1 TUTKIELMAN TAUSTAA	7
1.2 TAVOITTEET, TUTKIMUSONGELMAT JA RAJAUKSET.....	8
1.3 KESKEISET KÄSITTEET	9
1.4 TUTKIMUSMENETELMÄT JA -AINEISTOT.....	10
1.5 AIKAISEMPI TUTKIMUS	11
1.6 TEOREETTINEN VIITEKEHYS.....	13
1.7 TUTKIELMAN RAKENNE.....	14
2 VAKUUTUSPETOKSET ILMIÖNÄ	16
2.1 VAKUUTUSPETOSTEN YLEISKUVAUS.....	16
2.2 VAKUUTUSPROSESSI JA PETOSTEN SYNTYMEKANISMIT.....	17
2.3 VAKUUTUSPETOSTEN TYYPIT.....	19
2.4 VAKUUTUSPETOSTEN SEURAUKSET JA MERKITYS	21
2.5 VAKUUTUSPETOSTEN TUNNISTAMINEN JA ENNALTAEHKÄISY.....	22
2.6 TERVEYSVAKUUTUSPETOKSET	24
3 KONEOPPIMINEN OSANA VAKUUTUSPETOSTEN TUNNISTAMISTA JA ENNALTAEHKÄISYÄ	26
3.1 KONEOPPIMISEN PERIAATTEITA	26
3.2 KONEOPPIMINEN VAKUUTUSPETOSTEN TUNNISTAMISESSA	27
3.3 KESKEISET KONEOPPIMISMENETELMÄT VAKUUTUSPETOSTEN TUNNISTAMISESSA	28
3.4 KONEOPPIMISMENETELMIIN LIITTYVÄT HAASTEET JA RAJOITTEET	30
3.4.1 Teknisiin ja menetelmällisiin ratkaisuihin liittyvät haasteet ja rajoitteet	30
3.4.2 Eettiset ja yhteiskunnalliset haasteet ja rajoitteet	31
4 KONEOPPIMISEN ROOLI TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA	32
4.1 TUTKIMUSAINEISTON HANKINTA JA ESITTELY	32
4.2 TUTKIMUSAINEISTON ANALYYSI	36
4.3 KONEOPPIMISMENETELMIEN HYÖDYNTÄMINEN TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA.....	38
4.4 KONEOPPIMISMENETELMIEN KÄYTÖSSÄ HYÖDYNNETYT MENETELMÄT JA MUUTTUJAT	40
5 JOHTOPÄÄTÖKSET	43
5.1 KESKEISET TULOKSET.....	43
5.2 TUTKIMUKSEN ARVIOINTI JA JATKOTUTKIMUSEHDOTUKSET	45
LÄHDELUETTELO	47
4.4 KIRJALLISUUSLÄHTEET	47

4.5	VERKKOLÄHTEET	50
4.6	OIKEUDELLISET LÄHTEET	52

KUVIO- JA TAULUKKOLUETTELO

Kuvio 1. Teoreettinen viitekehys	13
Kuvio 2. Vakuutusprosessi	18
Kuvio 3. Systemaattisen kirjallisuuskatsauksen vaiheet (muk. Fink, 2019).....	32
Taulukko 1	33
Taulukko 2	35
Taulukko 3	36
Taulukko 4	37
Taulukko 5	37

lääketieteellisissä laskutustiedoissa erityisesti Yhdysvaltain Medicare –järjestelmässä. Suomessa aihetta ei kuitenkaan ole tutkittu akateemisesta näkökulmasta, eikä koneoppimisen roolia terveysvakuutuspetosten havaitsemisessa ole tarkasteltu kotimaisessa tutkimuskirjallisuudessa. Tämä muodostaa selkeän tutkimusaukon, jonka tarkastelu on merkityksellistä sekä vakuutusalan riskienhallinnan, korvausprosessien kehittämisen, että terveydenhuollon resurssien tehokkaan kohdentamisen kannalta.

1.2 Tavoitteet, tutkimusongelmat ja rajaukset

Tutkielman tavoitteena on selvittää, miten koneoppimismenetelmiä voidaan hyödyntää terveysvakuutuspetosten tunnistamisessa. Tutkielma pyrkii muodostamaan kokonaiskuvan koneoppimismenetelmien toimivuudesta, sekä arvioimaan niiden tarjoamia hyötyjä ja mahdollisuuksia vakuutusyhtiöiden riskienhallinnassa. Tutkielma pyrkii selvittämään erilaiset petostyypit, sekä kokoamaan tietoa erilaisten koneoppimismenetelmien soveltuvuudesta terveysvakuutuspetosten torjuntaan.

Tutkimusongelma voidaan kiteyttää seuraaviin tutkimuskysymyksiin:

1. Miten koneoppimismenetelmiä voidaan hyödyntää terveysvakuutuspetosten tunnistamisessa?
2. Millaisia menetelmiä ja muuttujia koneoppimismallit hyödyntävät tunnistamisprosessissa?

Tutkielma rajataan käsittelemään terveysvakuutuspetoksia, sillä niiden on osoitettu muodostavan merkittävän taloudellisen ja rakenteellisen haasteen vakuutusjärjestelmille. Kansainvälisten arvioiden mukaan terveydenhuollon laskutus- ja korvauspetoksista koituu vuosittain useiden prosenttien lisäkustannukset kokonaistason terveystalouteen, mikä heijastuu sekä vakuutusyhtiöiden taloudelliseen kantokykyyn että vakuutuksenottajien maksurasitteeseen (Dionne, Giuliano & Picard, 2009; Joudaki et al., 2015). Terveysvakuutuspetosten havaitsemista vaikeuttaa erityisesti niiden monimuotoisuus ja se, että petoksia voivat tehdä sekä palveluntuottajat että vakuutetut itse (Viaene & Dedene, 2004).

Rajauksen perusteltavuutta lisää myös se, että terveysvakuutusten tuottama data on määrällisesti laajaa ja rakenteeltaan koneoppimissovelluksille soveltuvaa, sillä korvaus- ja

laskutustapahtumat ovat hyvin dokumentoituja ja standardoituja (Bauder & Khoshgoftaar, 2018). Keskittymällä yhteen vakuutuslajiin mahdollistetaan ilmiön tarkempi analyysi, sillä vakuutuspetosten toimintalogiikka, petostyyppien esiintyvyys ja mallinnusmenetelmien soveltuvuus voivat vaihdella vakuutuslajin mukaan. Tämän rajauksen avulla tutkielma pyrkii syventämään ymmärrystä terveystakuutuspetosten erityispiirteistä ja arvioimaan koneoppimismenetelmien käyttöä niiden tunnistamisessa mahdollisimman systemaattisesti.

1.3 Keskeiset käsitteet

Tämä alaluku käsittelee tutkielmaan liittyviä keskeisiä käsitteitä, joiden avulla lukijan on mahdollista ymmärtää tutkittavaa aihetta paremmin. Käsitteiden määrittely on tärkeää, sillä ne muodostavat tutkimuksen teoreettisen pohjan.

Terveystakuutus on vakuutus, joka korvaa vakuutusehdoissa määritellyjä sairauksien ja tapaturmien hoitokuluja. Suomessa terveystakuutus on vapaaehtoinen ja sitä myöntävät yksityiset vakuutusyhtiöt. Sen tarkoitus on täydentää julkista terveydenhuoltoa ja nopeuttaa hoitoon pääsyä. Taloustieteellisesti terveystakuutus on riskienhallinnan väline, jossa riskiä jaetaan vakuutuksenottajien kesken vakuutusmaksuja vastaan (Rantala & Kivisaari, 2020, 56–57, 80; Outreville, 1998).

Vakuutuspetos on Suomen rikoslain mukaan teko, jossa henkilö pyrkii saamaan vakuutuskorvauksen syyttämällä palovakuutettua omaisuutta. Mikäli henkilö ei syyllisty samalla omaisuutta koskevaan petosrikokseen tai sellaisen yritykseen tuomitaan tämä vakuutuspetoksesta (RL, 36:4). Yleisesti kuitenkin vakuutuspetos täyttää petoksen tunnusmerkit sen osalta, että se siinä pyritään hankkimaan taloudellista hyötyä toista erehdyttämällä (RL, 36:1).

Tekoälyllä tarkoitetaan järjestelmiä, joilla pystytään suorittamaan ihmisen älykkyyttä, oppimista, päättelyä, kielen käsittelyä ja päätöksentekoa vaativia tehtäviä. Tekoälyn rooli liiketoiminnan eri osa-alueilla kasvaa nopeasti, ja sen avulla voidaan hallinnoida suuria tietomassoja, automatisoida rutiiniluontoisia tehtäviä ja parantaa asiakaspalvelukokemusta (Russell & Norvig, 2016).

Koneoppiminen on tekoälyn osa-alue, jossa järjestelmä oppii tunnistamaan kaavoja ja tekemään ennusteita historialliseen dataan peilaten ilman erillistä ohjelmointia (Goodfellow, Bengio & Courville, 2016).

1.4 Tutkimusmenetelmät ja -aineistot

Tutkielman tutkimusmenetelmäksi valikoitui laadullinen tutkimus systemaattisen kirjallisuuskatsauksen muodossa. Laadullisen tutkimuksen tavoitteena ei ole ensisijaisesti mitata ilmiöitä määrällisesti, vaan pyrkiä ymmärtämään niitä tulkinnan ja merkitysten kautta. Laadullinen tutkimus tarkastelee ilmiöitä kokonaisuutena ja pyrkii muodostamaan käsityksen siitä, miten ja miksi tarkasteltava ilmiö ilmenee tietyssä kontekstissa (Tuomi & Sarajärvi, 2018, 22–24). Tämän lähestymistavan valinta on perusteltu, sillä tutkielman tavoitteena on analysoida olemassa olevaa tutkimustietoa terveystieteen ja koneoppimismenetelmien suhteesta sekä tehdä näistä teemoista jäsennelty ja ymmärrettävä kokonaiskuva.

Kirjallisuuskatsauksia voidaan toteuttaa usein eri tavoin, kuten kuvailevina, integroivina, systemaattisina ja meta-analyyseina. Toteutustapaa valitessa sen tyyppi riippuu tutkimuskysymyksistä ja tavoitteista (Salminen, 2011). Systemaattisen kirjallisuuskatsauksen toteuttamisessa tärkeää on tutkimuskysymysten tarkka muotoilu, hakustrategian suunnittelu sekä hakuprosessin läpinäkyvyys ja kokonaisvaltainen raportointi. Kirjallisuuskatsauksen täytyy olla niin tarkasti dokumentoitu, että tutkimus on näiden ohjeiden perusteella toistettavissa (Salminen, 2011, 9–11).

Jotta tutkielma saatiin toteutettua systemaattisesti, valittiin sen toteuttamiseksi tarkat kriteerit sisäänoton ja poissulun osalta. Aineiston sisäänottoa rajattiin seuraavin kriteerein: vertaisarvioitu, englanninkielinen ja tutkii terveystieteen tunnistamista koneoppimisen avulla. Poissulun osalta kriteerinä oli, että artikkeleja, joissa käsitellään joitakin muita vakuutuslajeja ei oteta huomioon.

Hakuprosessi toteutettiin vaiheittain. Tutkielman aineistona käytetään vertaisarvioituja tieteellisiä artikkeleita. Aiheesta on saatavilla runsaasti kansainvälistä tutkimusta ja valittu aineisto on englanninkielistä suomenkielisen aineiston riittämättömyyden vuoksi. Aineisto on kerätty hakupalvelusta nimeltä Andor. Hakemiseen on hyödynnetty muun muassa

hakusanoja: *insurance fraud, health insurance fraud, machine learning in fraud detection, tekoäly vakuutuspetokset, terveystakuutuspetos ja koneoppiminen*. Näistä koottiin seuraava hakulauseke: ” (health OR medical) AND (fraud OR fraudulent) AND insurance AND machine learning”. Aineisto on rajattu vuosina 2020-2025 julkaistuun tutkimukseen, jotta se on mahdollisimman ajankohtaista olemassa olevaan tutkimukseen peilaten.

Lähteiden valinnassa on kiinnitetty huomiota niiden luotettavuuteen sekä siihen, että ne liittyvät mahdollisimman tiiviisti käsiteltävään tutkimusongelmaan. Tutkimus on rajattu siten, että se ei sisällä empiiristä aineistonkeruuta esimerkiksi haastatteluiden tai kyselyn muodossa. Sen sijaan empiriaosuuden aineiston keruu on toteutettu hyödyntämällä jo olemassa olevaa tieteellistä kirjallisuutta. Uuden tiedon keruun puuttumisen perustelen sillä, että tavoitteena on jäsenellä ja analysoida jo olemassa olevaa tutkimustietoa, jota on jo huomattava määrä. Lisäksi uuden aineiston keruu vakuutusyhtiöistä olisi käytännössä haastavaa aiheen luottamuksellisuuden ja arkaluonteisuuden vuoksi. Esimerkiksi haastattelu- tai kyselytutkimuksen toteuttaminen tässä kontekstissa voisi olla vaikeasti saavutettavaa ja rajallista.

Valitut artikkelit analysoidaan aineistolähtöisen sisällönanalyysin keinoin. Analyysissa keskitytään vertailemaan terveystakuutuspetosten tunnistamiseen ja ennaltaehkäisyyn käytettyjä koneoppimismenetelmiä, sekä tutkimaan millaisia etuja ja rajoitteita niihin liittyy. Analyysin tavoitteena on tuottaa kokonaiskuva koneoppimisen soveltamisesta vakuutuspetosten torjuntaan ja millaisia johtopäätöksiä tästä on mahdollista juontaa aiheen suomenkieliseen tutkimuskenttään.

1.5 Aikaisempi tutkimus

Vakuutuspetosten havaitsemista ja ennaltaehkäisyä on tutkittu kansainvälisesti useiden eri vakuutuslajien kontekstissa. Esimerkiksi Bolton ja Hand (2002) korostivat jo varhain 2000-luvun alussa, että perinteiset tilastolliset menetelmät ja sääntöpohjaiset järjestelmät ovat tehokas tapa vähentää petoksia, mutta petoksenteelijät kykenevät sopeutumaan tehokkaasti ja löytävät keinon kiertää tällaiset järjestelmät. Heidän mukaansa koneoppiminen tarjosi kuitenkin tehokkaan teknologian vakuutuspetosten havaitsemiseen.

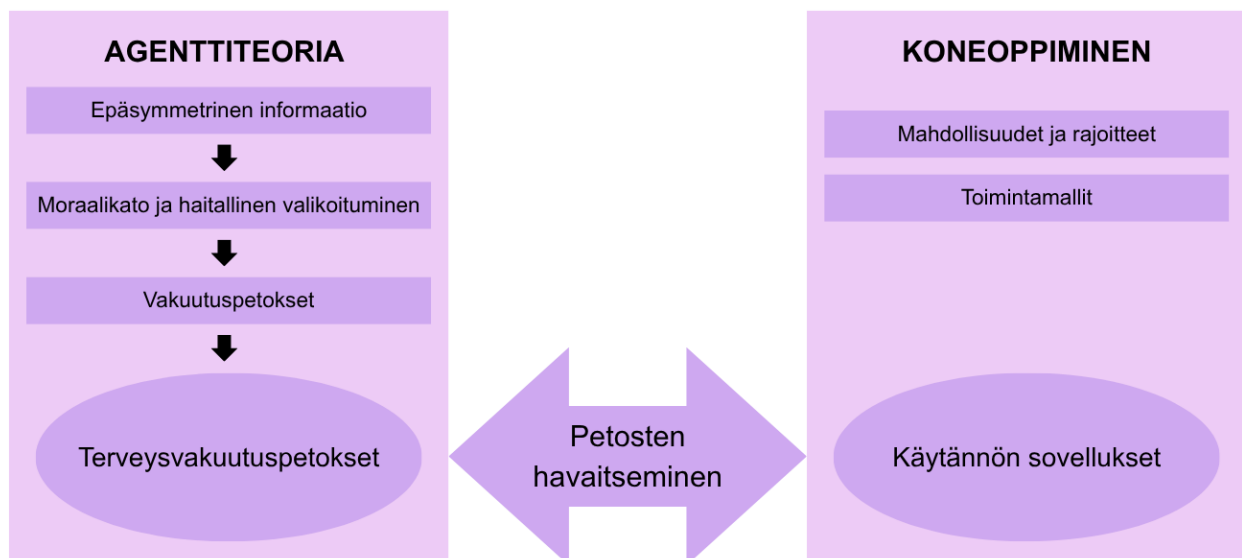
Terveysvakuutusten saralla tutkimusta on tehty erityisesti Yhdysvalloissa, jossa monimutkainen terveysvakuutusjärjestelmä, laaja yksityinen vakuutusmarkkina ja julkiset ohjelmat, kuten Medicare, luovat merkittäviä riskejä vakuutuspetoksille (Bauder et al., 2018; Shekhar, Leder-Luis et al., 2023). Viimeaikaisessa tutkimuksessa on korostunut erityisesti koneoppimismenetelmien hyödyntäminen petosten tunnistamisessa. Esimerkiksi Bauder et al. (2018) osoittavat tutkimukseen, että koneoppimismallit, kuten päätöspuut, neuroverkot ja erilaiset ensemble-mallit, voivat havaita terveysvakuutuspetoksiin viittaavia poikkeamia tarkemmin ja joustavammin kuin perinteiset sääntöpohjaiset valvontajärjestelmät.

Suomalaisessa tutkimuksessa koneoppimisen hyödyntämistä vakuutuspetoksiin on käsitelty hyvin vähän. Rantakangas (2021) tarkasteli pro gradu -tutkielmassaan dataa nimeämättömän vakuutusyhtiön henkilöasiakkaiden henkilö- ja pakettiautojen liikenteen omaisuuskorvauksista verraten perinteisiä tilastollisia malleja koneoppimismenetelmiin. Tutkimuksessa havaittiin, että koneoppimismallit tuottivat parempia tuloksia kuin perinteiset mallit. Jyrinsalo (2024) keskittyi kandidaatintutkielmassaan ajoneuvovakuutuspetosten havaitsemiseen teknologian avulla, tuoden esiin teknologisten ratkaisujen merkityksen petosten tunnistamisen tehostamisessa suomalaisessa toimintaympäristössä. Tukonen (2024) puolestaan tutki lohkoketjuteknologian roolia terveysvakuutuspetosten tunnistamisessa ja ehkäisyssä, ja korosti erityisesti tiedonvaihdon, läpinäkyvyyden ja tietoturvan merkitystä petosten torjunnassa. Näiden tutkimusten tulokset osoittavat, että myös Suomessa tunnistetaan digitaalisten teknologioiden ja dataperusteisen päätöksenteon kasvava merkitys vakuutusalan riskienhallinnassa.

Tämä kandidaatintutkielma täydentää aiempaa suomalaista tutkimusta tarkastelemalla tekoälyn ja koneoppimisen hyödyntämistä vakuutuspetosten ennaltaehkäisyssä sekä niiden tuomia mahdollisuuksia ja haasteita alan eettiselle ja operatiiviselle kehitykselle. Tutkielma pyrkii myös näyttämään, että koneoppimisen soveltamiselle vakuutuspetosten torjunnassa olisi paljon potentiaalia myös Suomessa, mutta näkökulmassa liittyen terveysvakuutuksiin on edelleen merkittävä tutkimusaukko.

1.6 Teoreettinen viitekehys

Tutkielman teoreettinen viitekehys (kuvio 1) rakentuu vakuutuspetoksia selittävän agenttiteorian sekä koneoppimisen tarjoamien käytännön sovellusten ympärille ja näitä kahta teemaa yhdistää terveysvakuutuspetosten tunnistaminen.



Kuvio 1. Teoreettinen viitekehys

Ensimmäinen teema käsittelee vakuutuspetoksia ja niiden syntymekanismeja. Vakuutuspetokset ovat olennainen osa vakuutusalan riskejä, ja niitä voidaan tarkastella agenttiteorian näkökulmasta. Agenttiteoriassa keskeinen ongelma on epäsymmetrinen informaatio vakuutuksenottajan (agentin) ja vakuutusyhtiön (päämiehen) välillä (Eisenhardt, 1989; Rothschild & Stiglitz, 1976). Tämä epäsymmetria luo kaksi merkittävää ilmiötä: moraalikadon ja haitallisen valikoitumisen (Arrow, 1963). Moraalikato ilmenee tilanteissa, joissa vakuutuksenottajan käyttäytyminen muuttuu vakuutuksen myötä riskialttiimmaksi tai opportunistiseksi, esimerkiksi liioiteltujen korvausvaatimusten muodossa. Haitallinen valikoituminen puolestaan tarkoittaa sitä, että vakuutuksen piiriin hakeutuu suhteessa enemmän korkean riskin yksilöitä, mikä vääristää vakuutusmaksujen tasapainoa ja heikentää riskipoolin kestävyttä. Molemmat ilmiöt altistavat järjestelmän vakuutuspetoksille, jotka heikentävät vakuutusjärjestelmän toimivuutta ja taloudellista kestävyttä.

Toinen teema keskittyy koneoppimiseen ja tekoälyyn terveystieteen tunnistamisen välineenä. Koneoppimisen avulla voidaan analysoida suuria tietomääriä ja tunnistaa monimutkaisia ja hienovaraisia käyttäytymismalleja tehokkaammin kuin perinteisillä tilastollisilla menetelmillä (Phua, Lee, Smith & Gayler, 2010). Koneoppimismallit, erityisesti luokittelu- ja poikkeavuuksien tunnistusmenetelmät, soveltuvat hyvin petosepäilyjen alustavaan tunnistamiseen. Menetelmien hyödyntämistä rajoittavat kuitenkin tietosuojan ja sääntelyyn liittyvät reunaehdot, kuten GDPR ja finanssivalvonnan ohjeistukset, jotka määrittävät, miten henkilötietoja ja potilastietoja voidaan käsitellä. Nämä sääntelykehykset, kuten myös riskienhallinnan kansainväliset standardit (esim. ISO 31000), luovat puitteet teknologian käytölle vakuutusalailla.

Näistä kahdesta keskeisestä teemasta muodostuu tutkielman teoreettinen viitekehys. Agenttiteoreettinen näkökulma tarjoaa perustan vakuutuspetosten dynamiikan ymmärtämiselle, kun taas koneoppimiseen liittyvä teoria avaa ne analyysimenetelmät, joita petosten tunnistamisessa voidaan hyödyntää. Näiden kahden teeman yhdistäminen luo pohjan tutkielman analyysille ja auttaa kytkemään teorian käytännön vakuutustoimintaan ja sen kehittämiseen.

1.7 Tutkielman rakenne

Tutkielman rakenne koostuu viidestä luvusta. Tutkielma alkaa johdannosta, jossa esitellään tutkielman aihe ja tavoite, keskeiset käsitteet ja teoreettinen viitekehys, tutkimuskysymykset ja -menetelmät sekä käytetty aineisto. Lisäksi johdannossa tiivistetään aiheeseen liittyvä aiempi tutkimus. Luku 2 on tutkielman ensimmäinen teorialuku, joka käsittelee vakuutuspetoksia. Siinä määritellään mitä vakuutuspetos tarkoittaa ja tarkastellaan eri petosmuotoja erityisesti terveystieteen osalta, sekä arvioidaan petosten vaikutuksia vakuutusjärjestelmään. Luku sisältää myös vakuutuspetosten tunnistamisprosessin tarkastelua. Luku 3 on tutkielman toinen teorialuku, joka keskittyy koneoppimismenetelmien ymmärtämiseen, sekä tarkastelee koneoppimisen roolia vakuutuspetosten torjunnassa.

Luku 4 sisältää tutkielman empiirisen osuuden, joka toteutetaan systemaattisena kirjallisuuskatsauksena. Empiirinen osuus sisältää tarkan kuvauksen aineistonkeruu- ja valintaprosessista, jonka jälkeen esitellään kirjallisuuskatsauksen tutkimustulokset ja aineistoon pohjautuva analyysi. Tutkielman viimeinen osa on luku 5, joka sisältää tutkielman

johtopäätökset. Se nitoo yhteen keskeiset havainnot, vastaa asetettuihin tutkimuskysymyksiin ja arvioi tutkimuksen luotettavuutta. Lisäksi luvussa 5 esitetään suosituksia aiheeseen liittyvälle jatkotutkimukselle.

2 VAKUUTUSPETOKSET ILMIÖNÄ

2.1 Vakuutuspetosten yleiskuvaus

Vakuutuspetos on tilanne, jossa vakuutuksenottaja tai muu osapuoli pyrkii perusteettomasti saamaan vakuutuksestaan taloudellista hyötyä vakuutusyhtiöltä erehdyttämällä tätä (RL 36:4§, RL 36:1§; Interpol 2021). Vakuutuspetos on Suomen rikoslain mukaan rangaistava teko, joka voidaan luokitella perusmuotoiseksi tai törkeäksi petokseksi teon vakavuuden perusteella (RL 36:1§). Vakuutuspetokset kuuluvat talousrikollisuuden piiriin ja ovat kansainvälisesti merkittävä rikollisuuden muoto (Interpol, 2021).

Vakuutuspetoksia voidaan tarkastella myös taloustieteen ja agenttiteorian näkökulmasta. Vakuutusyhtiö toimii päämiehenä, joka tarjoaa vakuutuksenottajalle palvelua, jossa yhtiö kantaa vakuutuksenottajan riskin. Koska vakuutusyhtiöllä on rajoitettu pääsy vakuutuksenottajan yksityisiin tietoihin ja käyttäytymiseen, syntyy epäsymmetrisen informaation tilanne. Rothschild ja Stiglitz (1976) ovat osoittaneet, että tällainen informaation epäsymmetria voi johtaa epävakaaseen tasapainoon vakuutusmarkkinoilla, jossa vakuutuksen hinnoittelu vääristyy, ja markkinoille syntyy moraalikatoa. Moraalikato on tilanne, jossa vakuutuksenottajalla on edellytykset liioitella vahinkoja tai toimia riskialttiimmin, koska hän tietää vakuutuksen kattavan kustannukset (Rothschild ja Stiglitz, 1976).

Empiiristä näyttöä tästä tarjoaa Cummins ja Tennyson (1996), joiden tutkimus autovakuutuksista osoitti, että osa vakuutetuista käyttäytyy tilaisuuden tullen systemaattisesti, esimerkiksi liioittelemalla vahinkoja korvaushakemuksissa. Tämä vahvistaa käsitystä siitä, että moraalikato ei ole vain teoria, vaan todellinen ilmiö, joka näkyy vahvasti vakuutusmarkkinoilla ja kasvattaa yhtiöiden korvauskuluja.

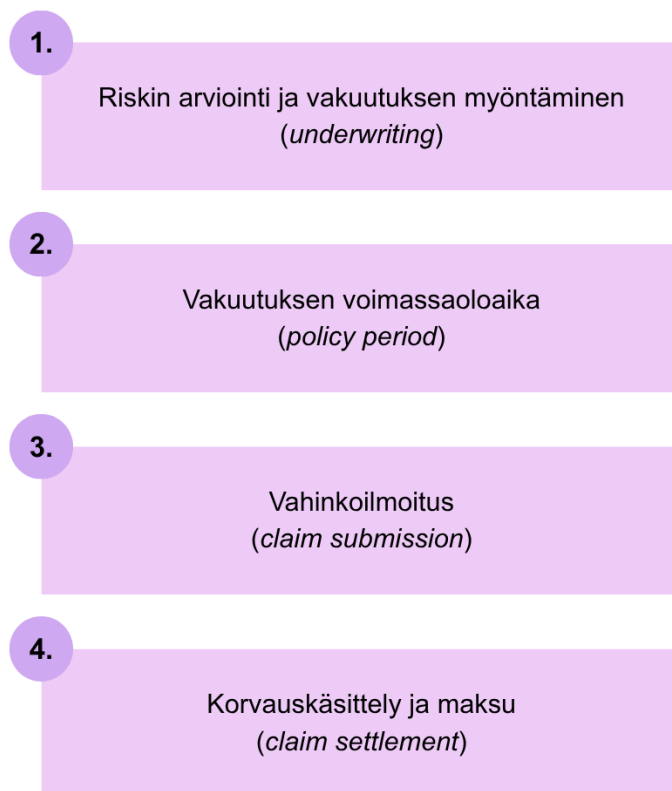
Vakuutuspetokset ovat talouden näkökulmasta tarkasteltuna erittäin merkittävä ongelma. Esimerkiksi Euroopassa vakuutuspetosten aiheuttamat kustannukset voivat olla jopa kymmenen prosenttia kaikista korvauskuluista (Insurance Europe, 2024). Suomen kontekstissa on arvioitu, että vakuutusyhtiöille on ilmoitettu vuositasona tuhansia petosepäilyjä, joiden kokonaisarvo on toista sataa miljoonaa euroa (Finanssiala ry, 2023).

Vakuutuspetosten aiheuttamat kustannukset eivät jää ainoastaan vakuutusyhtiöiden tappioiksi, vaan niistä aiheutuvat kustannukset heijastuvat myös vakuutuksenottajien kustannuksissa kohonneina vakuutusmaksuina (Finanssiala ry, 2023; Insurance Europe, 2019).

Vakuutuspetokset ovat ilmiönä erittäin monimuotoinen. Petoksia voi esiintyä esimerkiksi pieninä väärinkäytöksinä, kuten vahingon liiotteluna tai olemattoman vahingon ilmoittamisena. Toisaalta petokset voivat olla myös laajamittaisia ja jopa järjestelmällisiä, jolloin niihin voi liittyä myös organisoitua rikollisuutta (Derrig, 2002; Button & Gee, 2013). Lisäksi vakuutuspetoksiin liittyy usein niin sanottu ”harmaa alue”, jossa virheen ja vilpin välinen ero on epäselvä. Kaikki väärät ilmoitukset eivät välttämättä ole tarkoituksellisia, vaan voivat johtua esimerkiksi tulkintaeroista vakuutusehdoissa, mikä tekee petosten tunnistamisesta erityisen haastavaa (Gee & Button, 2019).

2.2 Vakuutusprosessi ja petosten syntymekanismit

Vakuutustoiminta perustuu riskien yhteisölliseen jakamiseen vakuutuksenottajien ja vakuutusyhtiön välillä. Tätä toimintaa voidaan kuvata vakuutusprosessina (kuvio 2), joka kattaa keskeiset vaiheet riskin arvioinnista korvausten käsittelyyn (Outreville, 1998). Prosessin eri vaiheissa syntyy mahdollisuuksia väärinkäytöksille, ja siksi petosten tunnistaminen edellyttää koko prosessin ymmärtämistä. Vakuutusprosessi jaetaan tyypillisesti neljään vaiheeseen.



Kuvio 2. Vakuutusprosessi

Riskin arviointi ja vakuutuksen myöntäminen (*underwriting*): Tässä vaiheessa vakuutusyhtiö arvioi asiakkaan riskiprofiilin ja hinnoittelee vakuutuksen sen perusteella. Petosriski voi syntyä, jos asiakas antaa tahallisesti virheellisiä tietoja esimerkiksi terveydentilastaan tai omaisuutensa arvosta (Rothschild & Stiglitz, 1976; Dionne, 2013).

Vakuutuksen voimassaoloaika (*policy period*): Riskiprofiili voi muuttua ajan kuluessa, mutta jos muutoksista ei ilmoiteta, syntyy informaation epäsymmetriaa, joka voi johtaa moraalikattoon (Cummins & Tennyson, 1996; Picard, 2000).

Vahinkoilmoitus (*claim submission*): Tämä on vakuutusprosessin kriittisin vaihe petosten kannalta, sillä suurin osa vakuutuspetoksista tapahtuu korvausvaiheessa (Derrig, 2002; Viaene & Dedene, 2004). Vahinkoilmoituksia voidaan vääristää esimerkiksi liioittelemalla vahingon laajuutta tai ilmoittamalla olemattomia vahinkoja.

Korvauskäsittely ja maksu (*claim settlement*): Tässä vaiheessa vakuutusyhtiö arvioi korvausvaatimuksen perusteet ja tekee maksupäätöksen. Petosten havaitseminen on tässä vaiheessa mahdollista dataperusteisesti, esimerkiksi koneoppimismallien avulla, jotka tunnistavat poikkeavia vahinkomalleja tai epätyypillistä käyttäytymistä (Viaene & Dedene, 2004).

Kokonaisuutena vakuutusprosessi muodostaa monivaiheisen riskienhallintaketjun, jossa informaatio kulkee useiden osapuolten kautta. Epäsymmetrinen informaatio ja inhimillinen harkinta luovat haavoittuvuuksia, joita petolliset toimijat voivat hyödyntää (Rothschild & Stiglitz, 1976). Teknologinen kehitys, erityisesti koneoppiminen ja tekoäly ovat tuoneet uusia keinoja valvoa ja analysoida prosessin eri vaiheita, mikä mahdollistaa petosten ennaltaehkäisyn entistä aikaisemmassa vaiheessa.

2.3 Vakuutuspetosten tyypit

Vakuutuspetokset voidaan jaotella usealla eri tavalla. Viaene ja Dedene (2004) määrittelevät vakuutuspetoksen sellaiseksi toiminnaksi, jossa yksi vääristää tahallisesti tietoja vakuutukseen liittyen saadakseen perusteetonta taloudellista hyötyä vakuutus sopimukseen vedoten. Heidän mukaansa vakuutuspetoksen tunnusmerkkeihin sisältyy väärän tiedon antamista, vilpillistä toimintaa, sekä pyrkimys saavuttaa etua, johon ei ole oikeutettu.

Yksinkertaisin tapa erottaa vakuutuspetokset on jakaa ne ulkoisiin ja sisäisiin petoksiin riippuen siitä, kuka petoksen suorittaa. Ulkoinen petos on yleisin vakuutuspetosten muoto, ja se kohdistuu yhtiöön vakuutuksenhakijan tai korvauksenhakijan taholta, kun taas sisäinen petos tapahtuu vakuutusorganisaation sisällä, esimerkiksi työntekijän väärinkäytöksen seurauksena. (Viaene & Dedene, 2004, 316) Ulkoiset petokset perustuvat usein väriin tietoihin, olemattomiin vahinkoihin tai liioiteltuihin korvausvaatimuksiin (Viaene & Dedene, 2004, 316; IAIS, 2021). Sisäiset petokset puolestaan liittyvät vakuutusyhtiön sisällä tapahtuvaan toimintaan, esimerkiksi työntekijöiden tai yhteistyökumppaneiden vilpilliseen toimintaan, kuten korvausten manipulointiin tai asiakastietojen väärinkäyttöön. Sisäiset petokset ovat vakava ongelma, sillä sisäistä petosta voi esiintyä kaikilla organisaatiotasolla, myös hallituksen ja ylimmän johdon tasolla. Mitä ylemmällä tasolla petos tapahtuu, sitä suurempi on todennäköinen taloudellinen tappio ja mainehaitta. (IAIS, 2021)

Toinen yleinen tapa luokitella vakuutuspetoksia on jakaa ne pehmeisiin (*soft fraud*) ja koviin (*hard fraud*) petoksiin. Pehmeälle petokselle on ominaista opportunistinen toiminta, jossa vakuutettu hyödyntää tilannetta saadakseen perusteetonta taloudellista hyötyä. Tyypillinen esimerkki tästä on korvaussumman liioittelu todellista vahinkoa suuremmaksi. Kova petos sen sijaan on suunnitelmallinen ja usein organisoitu teko, jossa toiminta on etukäteen harkittua ja toistuvaa. Kovissa petoksissa voi esiintyä esimerkiksi lavastettuja onnettomuuksia, tekaistuja vahinkoja tai väärennettyjä asiakirjoja. (Viaene & Dedene, 2004; Derrig, 2002)

Petokset on mahdollista jakaa myös vakuutuksen elinkaaren mukaan kahteen luokkaan, jotka liittyvät vakuutuksen myöntämiseen (*underwriting fraud*), sekä korvausvaiheeseen (*claims fraud*). Vakuutuksen myöntämiseen liittyvät petokset liittyvät esimerkiksi väärin tietoihin jo vakuutusta hakiessa tai vaihtoehtoisesti riskin tahalliseen aliarviointiin. Korvausvaiheen petoksiin puolestaan liittyy liiotellut, virheelliset tai keksityt vahinkoilmoitukset. (Viaene & Dedene, 2004, 316)

Vakuutuspetoksia esiintyy jokaisessa vakuutuslajissa, mutta niiden yleisyys ja ilmenemismuodot vaihtelevat. Esimerkiksi liikennevakuutuksessa tyypillisiä ovat lavastetut onnettomuudet ja vahinkojen liioittelu (Derrig, 2002), kun puolestaan terveystakuutuksissa esiintyy myös palveluntarjoajien tekemiä väärinkäytöksiä, kuten olemattomien palveluiden laskuttamista tai hoitotoimenpiteiden tarpeettomaksi paisuttelua (Gee & Button, 2019; NHCAA, 2019).

Vakuutuspetosten eroavaisuudet osoittavat, että ilmiö ei rajoitu yksittäisiin vakuutuslajeihin tai toimintatapoihin, vaan siihen liittyy sekä yksilöiden, että organisaatioiden väärinkäytöksiä. Pehmeät ja kovat petokset muodostavat kokonaisuuden, jossa motiivit vaihtelevat taloudellisesta ahdingosta systemaattiseen rikolliseen toimintaan (Derrig, 2002; IAIS, 2021). Petosten monimuotoisuus vaikeuttaa niiden havaitsemista ja luokittelua, mikä korostaa valvonnan ja analytiikan merkitystä. Näin ollen vakuutuspetosten torjunta edellyttää kokonaisvaltaista lähestymistapaa, jossa huomioidaan sekä inhimillisyys että teknologiset tekijät, kuten riskienhallinta, data-analytiikka ja viranomaisyhteistyö (IAIS, 2021).

2.4 Vakuutuspetosten seuraukset ja merkitys

Vakuutuspetokset aiheuttavat huomattavia haittoja sekä pelkästään vakuutusyhtiöille että koko yhteiskunnalle (ks. Finanssiala ry, 2023). Taloudellisesta näkökulmasta petokset heikentävät vakuutusjärjestelmän tehokkuutta, vääristävät vakuutustuotteiden hinnoittelua ja siirtävät kustannuksia rehellisille vakuutuksenottajille. Cummins ja Tennyson (1996) osoittivat tutkimuksessaan ajoneuvovakuutuspetoksista, että vakuutuspetokset lisäävät vakuutusyhtiöiden korvauskustannuksia ja johtavat moraalikadon voimistumiseen erityisesti ajoneuvovakuutuksissa. Näiden ylimääräisten kustannusten seurauksena vakuutusmaksut nousevat jokaisen asiakkaan kohdalla ja tämä heikentää järjestelmän oikeudenmukaisuutta.

Taloudelliset vaikutukset ovat huomattavia. Suomessa Finanssiala ry (2023) arvioi, että yhtiöt tunnistavat vuosittain tuhansia petosepäilyjä, yhteisarvoltaan yli sata miljoonaa euroa. Isossa-Britanniassa ABI raportoi tuoreissa tilastoissaan kymmeniä tuhansia paljastettuja petoksia ja yli miljardin punnan kokonaissummia raportointivuotenaan (ABI, 2022).

Laajemmin tarkasteltuna vakuutuspetokset heikentävät vakuutusjärjestelmän peruseriaatetta, eli riskin jakamista vakuutuksenottajien kesken. Kun osa toimijoista väärinkäyttää järjestelmää, syntyy epäsymmetrisen informaation ongelmia ja luottamuksen heikkenemistä vakuutusyhtiöiden ja asiakkaiden välillä. Rothschildin ja Stiglitzin (1976) klassinen epätäydellisen informaation teoria osoittaa, että epäsymmetrinen informaatio voi johtaa haitalliseen valikoitumiseen, jossa matalariskiset vakuutuksenottajat poistuvat markkinoilta korkeariskisten vakuutustenottajien aiheuttamien vakuutusmaksujen noustessa. Pitkällä aikavälillä tämä voi horjuttaa koko vakuutusjärjestelmän kestävyyttä (Cummins & Tennyson, 1996).

Vakuutuspetoksilla on myös merkittäviä eettisiä ja yhteiskunnallisia vaikutuksia. Button, Johnston ja Frimpong (2013, 25–27) korostavat, että vakuutuspetokset eivät ole ainoastaan talousrikoksia, vaan ne myös rapauttavat moraalista luottamusta ja yhteiskunnan normeja. Derrig (2002) toteaa, että vakuutuspetokset voivat johtaa tilanteeseen, jossa poikkeavuus alkaa normalisoitumaan ja osa kuluttajista alkaa pitää petoksia oikeutettuina. Tämän myötä pienet epärehellisyydet alkavat saada hyväksyntää, joka puolestaan heikentää vakuutusjärjestelmän sosiaalista legitimitettä. Petokset vahingoittavat yleisesti koko

vakuutusalan mainetta ja voivat näin ollen vähentää kuluttajien halukkuutta hankkia vakuutuksia, joka puolestaan heikentää riskienhallinnan kattavuutta koko yhteiskunnassa.

Lisäksi vakuutuspetokset vaikuttavat suoraan sääntely- ja valvontaympäristöön. Vakuutuspetosten ehkäisy ja tunnistaminen lisäävät tarkastus- ja raportointivelvoitteita, mikä kasvattaa vakuutusyhtiöiden hallinnollista kuormaa ja kustannuksia (Derrig, 2002, 278–280). Finanssivalvonta (2024) on puolestaan painottanut hallinnon ja sisäisen valvonnan kehittämistä vakuutussektorilla petosten ehkäisemiseksi. Tämä kertoo siitä, että vakuutuspetokset eivät ole pelkästään liiketoiminnallinen riski, vaan myös sääntelyyn ja valvontaan vaikuttava ilmiö.

Yhteenvetona voidaan todeta, että vakuutuspetokset eivät ole vain yksittäisiä talousrikkomuksia, vaan ne muodostavat moniulotteisen yhteiskunnallisen ja taloudellisen ongelman. Petokset heikentävät vakuutusjärjestelmän tehokkuutta, oikeudenmukaisuutta ja legitimitteettiä, kasvattavat rehellisten asiakkaiden taloudellista taakkaa sekä lisäävät yleistä sääntelypainetta ja hallinnollisia kustannuksia. Näiden asioiden vuoksi vakuutuspetosten tunnistaminen on keskeinen tekijä vakuutusalan kestävyiden turvaamisessa.

2.5 Vakuutuspetosten tunnistaminen ja ennaltaehkäisy

Vakuutuspetosten tehokas tunnistaminen perustuu sekä teknologisiin menetelmiin että organisaation sisäisiin toimintatapoihin, kuten valvontaan ja henkilöstön koulutukseen. Cummins ja Tennyson (1996) korostavat, että vakuutuspetosten torjunta edellyttää tasapainoa tehokkuuden ja asiakaskokemuksen välillä. Liiallinen valvonta voi heikentää asiakasluottamusta, kun taas liian löysä ote puolestaan lisää väärinkäytösten riskiä. Perinteisesti vakuutusyhtiöt ovat hyödyntäneet tilastollisia ja sääntöpohjaisia menetelmiä petosten havaitsemisessa. Näissä menetelmissä epäilyttävä toiminta määritellään ennalta asetettujen kriteerien perusteella, mikä tekee niistä jäykkiä ja usein tehottomia muuttuvien petosmallien tunnistamisessa (Bolton & Hand, 2002, 236–238). Näitä ovat muun muassa poikkeavuuksien tunnistus, uusien korvausilmoitusten vertailu historiadatan kanssa sekä asiantuntijoiden tekemä riskiluokittelu (Derrig, 2002, 271–279). Vaikka näitä perinteisiä menetelmiä käytetään edelleen, eivät ne kykene välttämättä tunnistamaan uusia monimutkaisia petosmuotoja.

Digitalisaatio ja datan saatavuuden kasvu ovat mahdollistaneet merkittäviä edistysaskeleita petosten torjunnassa. Infosys on globaali IT-konsultoinnin ja teknologiapalveluiden yritys, joka tuottaa analyyseja ja ratkaisuja muun muassa vakuutusalan digitalisaatiosta. Infosysin (2023) mukaan tekoälyyn ja koneoppimiseen perustuvat mallit ovat muuttaneet vakuutuspetosten havaitsemista reaktiivisesta toiminnasta ennakoivaksi. Ennustavat mallit pystyvät tunnistamaan poikkeavia käyttäytymismalleja ja epäilyttäviä kuvioita jo ennen kuin vahinko tapahtuu. Chyn (2024) tutkimuksen mukaan koneoppimisen avulla petoksista on mahdollista oppia jatkuvasti ja tätä kautta mukautua uusiin ilmiöihin, joka vähentää väärin hälytysten määrää ja parantaa tunnistustarkkuutta.

Vakuutuspetosten ennaltaehkäisy ei kuitenkaan ole pelkästään tekninen kysymys, vaan se vaatii kokonaisvaltaista lähestymistapaa, jossa yhdistyvät teknologia, hallinto ja etiikka. Finanssivalvonnan (2024) mukaan sisäisen valvonnan vahvistaminen, henkilöstön koulutus sekä yrityskulttuuri, joka painottaa eettisyyttä ja avoimuutta, ovat kaikki olennaisia tekijöitä petosten ehkäisyssä. Samoin asiakkaiden tietoisuuden lisääminen ja avoin viestintä petosten seurauksista voivat vähentää niiden hyväksyttävyyttä (Button et al., 2013).

Käytännössä tehokas petostorjunta perustuu monikerroksiseen malliin, jossa yhdistyvät erilaiset järjestelmät, asiantuntijoiden arviot, sekä viranomaisyhteistyö. Insurance Fraud Bureau (2024; 2025) korostaa tiedonvaihdon merkitystä eri toimijoiden välillä, sillä monet petokset paljastuvat vasta, kun eri vakuutusyhtiöiden tietoja yhdistetään toisiinsa. Tämän vuoksi tietosuojan ja tietojen vastuulliseen käsittelyyn liittyvät sääntelyvaatimukset, kuten yleinen Euroopan unionin tietosuoja-asetus GDPR (EU 2016/679), ovat keskeisiä myös petosten torjunnassa.

Perinteiset sääntöpohjaiset menetelmät ja asiantuntijapohjainen tapauskohtainen arviointi ovat edelleen tärkeitä, mutta niillä on rajoitteensa: ne vaativat manuaalista työtä, ne eivät välttämättä skaalaudu suuriin datamassoihin, ja ne voivat olla hitaita mukautumaan uusiin petosmalleihin (Derrig, 2002, 271–279). Tästä syystä vakuutusala on siirtynyt yhä enemmän kohti datavetoisia menetelmiä, jotka hyödyntävät tilastollista mallinnusta ja koneoppimista. Koneoppimisen etuna on se, että mallit voidaan kouluttaa havaitsemaan sekä aiemmin tunnettujen petostapausten kaltaisia rakenteita että täysin uusia, poikkeavia toimintamalleja. Koneoppimista hyödynnetään erityisesti korvausvaiheen petosten tunnistamisessa, sillä

juuri tämä vaihe on alttiimpi väärinkäytöksille monimutkaisten laskutusprosessien ja toimijoiden suuren määrän vuoksi. (Bauder, Khoshgoftaar & Richter, 2017, 3–6)

Yhteenvedona voidaan todeta, että vakuutuspetosten tunnistaminen ja ennaltaehkäisy edellyttävät tasapainoa teknologian ja eettisen vastuun välillä. Tekoäly ja koneoppiminen tarjoavat lupaavia välineitä petosten havaitsemiseen, mutta niiden rinnalla tarvitaan vahvaa hallintoa, eettistä johtamista ja eri tahojen välistä yhteistyötä.

2.6 Terveysvakuutuspetokset

Terveysvakuutuspetokset muodostavat merkittävän osan vakuutuspetoksista (Gee & Button, 2019). Terveysvakuutuspetokset sisältävät laajan kirjon erilaisia toimintatapoja, kuten olemattomien potilaiden laskuttamista, tarpeettomien toimenpiteiden toteuttamista ja monimuotoista liiottelua (Gee & Button, 2019). Petoksiin voi liittyä myös palvelujen väärää esittämistä tai kokonaan toteutumattomien palveluiden laskuttamista (Derrig, 2002).

Kansainvälisesti terveystakuutuspetosten mittakaava on huomattava ja sen taloudelliset vaikutukset ovat merkittäviä. Gee ja Button (2015) tarkastelivat laajassa tutkimuksessaan 33 terveystakuutusorganisaatiota seitsemästä eri maasta ja pyrkivät arvioimaan petosten aiheuttamaa rasitusta terveydenhuollon kokonaismenoihin. Tutkimuksen perusteella vuosien 1997–2013 aikana petosten aiheuttama keskimääräinen menojen menetys oli 6,19 prosenttia (Gee & Button, 2015). Tämä prosenttiosuus ei ole pelkästään abstrakti luku, vaan se konkretisoituu valtavina taloudellisina menetyksinä. Esimerkiksi vuonna 2013 arvioitiin, että maailmanlaajuisissa terveydenhuoltomenoissa menetettiin petosten seurauksena noin 455 miljardia dollaria eli 350 miljardia euroa (Gee & Button, 2015). Kyseessä on summa, joka vastaa monien valtioiden koko terveydenhuollon vuosibudjettia ja joka osoittaa, kuinka laajalle levinnyt ja vakava ongelma terveystakuutuspetokset ovat globaalilla tasolla.

Geen ja Buttonin (2015) analyysi tuo esiin sen, että petosten vaikutukset eivät rajoitu yksittäisiin vakuutusyhtiöihin tai kansallisiin järjestelmiin, vaan ne heijastuvat koko terveydenhuollon ekosysteemiin, jossa kustannusten kasvu kohdistuu lopulta myös vakuutuksenottajiin ja potilaisiin, sillä petosten aiheuttamat menetykset kompensoidaan usein korkeampina vakuutusmaksuina tai rajoituksina palveluiden saatavuudessa. Lisäksi tutkimus korostaa, että petosten mittakaava on pysynyt merkittävänä pitkällä aikavälillä,

mikä viittaa siihen, että ongelma ei ole hetkellinen poikkeama vaan rakenteellinen haaste, joka edellyttää jatkuvaa valvontaa ja kehittyneitä havaitsemismenetelmiä. Näin ollen Geen ja Buttonin (2015) esittämät luvut tarjoavat vahvan perustan ymmärtää, miksi terveysvakuutuspetosten torjunta on keskeinen osa sekä kansallista että kansainvälistä terveydenhuollon ja vakuutustoiminnan kehittämistä.

Terveysvakuutuspetokset eroavat muista vakuutuspetoksista siten, että niihin voi osallistua myös palveluntarjoajat, kuten lääkärit ja heidän työnantajansa (Gee & Button, 2019). Lisäksi ilmiöön liittyy usein harmaa alue, jossa virheen ja vilpin erottamisesta tulee epäselvää, joka tekee terveysvakuutuspetosten tunnistamisesta erityisen haastavaa (Button & Gee, 2013). Palveluntarjoajapetoksissa tyypillisiä muotoja ovat *upcoding* (kalliimman toimenpidekoodin laskutus), *unbundling* (pakettitoimenpiteiden pilkkominen erillisiksi korvattaviksi toimenpiteiksi), *phantom billing* (olemattomien potilaiden tai palvelujen laskutus) sekä tarpeettomien toimenpiteiden toteuttaminen. Nämä käytännöt on dokumentoitu terveyssektorin kansainvälisissä katsauksissa ja raporteissa. (Gee & Button, 2019; Derrig, 2002)

Yhteenvetona voidaan todeta, että terveysvakuutuspetokset ovat globaalisti miljardiluokan ongelma, jonka monimuotoisuus ja palveluntarjoajien osallisuus tekevät niiden torjunnasta haastavaa. Koska perinteiset menetelmät eivät riitä havaitsemaan kaikkia petosmuotoja, koneoppimisen hyödyntäminen tarjoaa uudenlaisen mahdollisuuden tunnistaa poikkeamia ja tehostaa valvontaa. Seuraavassa luvussa tarkastellaan, miten koneoppimismenetelmiä on sovellettu tämän ongelman ratkaisemiseksi.

3 KONEOPPIMINEN OSANA VAKUUTUSPETOSTEN TUNNISTAMISTA JA ENNALTAEHKÄISYÄ

3.1 Koneoppimisen periaatteita

Koneoppiminen (engl. *machine learning, ML*) on tekoälyn osa-alue, jossa tietokoneohjelma oppii toimimaan tehokkaammin sille syötetyn datan avulla ilman, että se on erikseen ohjelmoitu jotakin tiettyä ratkaisua varten (Mitchell, 1997, 2). Koneoppiminen nähdään usein jatkumona tilastollisille menetelmille. Koneoppiminen kuitenkin eroaa perinteisistä tilastollisista menetelmistä siten, että sillä on kyky käsitellä suuria määriä dataa, sekä löytää piileviä rakenteita, joita olisi hankala havaita perinteisin menetelmin (Hastie, Tibshirani & Friedman, 2009, 1–3).

Yleisesti koneoppimisen menetelmät jaetaan yleisesti neljään ryhmään:

1. *Valvottu oppiminen* (supervised learning), jossa tekoälyä opetetaan esimerkkien avulla. Syötteen ja tavoitteen välisestä suhteesta opitaan funktio, jota voidaan hyödyntää uusissa havainnoissa. Tyypillisiä valvotun oppimisen sovelluksia ovat luokittelu ja regressio (Murphy, 2012, 2–3). Esimerkiksi jos vakuutusyhtiöllä on historiatietoa paljastuneista petostapauksista, voidaan näiden avulla kouluttaa luokittelija, joka oppii tunnistamaan samanlaisia tapauksia jatkossa.
2. *Valvomaton oppiminen* (unsupervised learning), jossa tekoälyn tavoitteena on löytää rakenteita ilman sille ennalta määriteltyjä vastauksia. Esimerkkejä tästä on klusterointi ja anomalioiden tunnistus (Bishop, 2006, 423). Käytännössä valvomaton oppimista voidaan hyödyntää esimerkiksi havaitsemaan epätavallista toimintaa perustuen esimerkiksi käyttäytymisprofiileihin tai laskutusrutiineihin.
3. *Puoliöhjattu oppiminen* (semi-supervised learning) sijoittuu valvotun ja valvomattoman oppimisen väliin. Puoliöhjattu oppiminen toimii siten, että pieni määrä luokiteltua dataa yhdistetään suurem määrään luokittelematonta dataa. Tällä tavoin mallin suorituskykyä saadaan parannettua (Zhu & Goldberg, 2009, 1–3). Tämä on hyödyllistä erityisesti tilanteissa, jossa luokitellun datan hankkiminen on todella kallista tai hidasta, mutta raakadataa on saatavilla runsaasti. Tämä menetelmä

soveltuu hyvin esimerkiksi vakuutuspetosten torjuntaan, jossa varmoja petoksia on vain murto-osa kaikista havainnoista. Puoliohjattua oppimista voidaan käyttää esimerkiksi terveysvakuutuspetosten tunnistamiseen, sillä varmistettuja petostapauksia on datamäärään nähden vähän ja puolestaan raakadataa on tarjolla runsaasti.

4. *Vahvistusoppiminen* (reinforcement learning), jossa tekoäly oppii toimimaan kokeilun ja palautteen avulla. Kone testaa erilaisia ratkaisuja ja saa niistä palautetta, sekä palkkion tai rangaistuksen. Tavoitteena kouluttaa kone löytämään sellaisia ratkaisuja, jotka pitkällä aikavälillä tuottavat suurimman hyödyn (Sutton & Barto, 2018, 1). Vahvistusoppimismalli voi esimerkiksi oppia, millaiset tapaukset tulisi ohjata ihmiselle tarkempaan arviointiin. Tässäkin tavoitteena on vahvistusoppimismallille tyypillisesti löytää toimintamalli, joka maksimoi petosten havaitsemisen ja minimoi turhat tutkintapyynnöt.

Koneoppimisen soveltuvuus vakuutuspetosten tunnistamiseen perustuu sen kykyyn käsitellä ja analysoida suuria määriä dataa, joissa petokset ovat harvinaisia. Valvomattomilla menetelmillä voidaan havaita poikkeavia tapahtumia, kun taas valvotut menetelmät mahdollistavat sellaisten mallien kehittelyn, jotka ovat oppineet aiemmin tunnistetuista petostapauksista. (Alpaydin, 2021, 13, 442) Näiden ominaisuuksien vuoksi koneoppiminen on noussut keskeiseksi työkaluksi vakuutuspetosten torjunnassa, sillä se tarjoaa perinteisiä menetelmiä tehokkaampia ratkaisuja (Russell & Norvig, 2016, 699–701).

3.2 Koneoppiminen vakuutuspetosten tunnistamisessa

Tässä alaluvussa kuvataan koneoppimismenetelmien roolia ja teoriaa vakuutuspetosten tunnistamisessa. Vakuutuspetosten havaitseminen on haastavaa, sillä petostapaukset ovat harvinaisia ja monimuotoisia verrattuna normaaleihin vakuutuskorvauksiin (Insurance Europe, 2019). Petosten havaitseminen on aiemmin perustunut pääosin perinteisiin menetelmiin, jotka ovat kalliimpia ja tehottomampia kuin koneoppimismenetelmät. Tästä syystä koneoppimisen rooli vakuutuspetosten tunnistamisessa on kasvanut, koska menetelmät ovat tehokkaampia, sekä pysyvät paremmin aallonharjalla muuttuvien petosmuotojen tunnistamisessa. (Russell & Norvig, 2016)

Vakuutusalan kontekstissa koneoppimista voidaan hyödyntää erityisesti anomaliatunnistuksessa, jossa tavoitteena on havaita poikkeavia korvaushakemuksia, sekä valvotun oppimisen kautta, jossa tavoitteena on kouluttaa tekoäly oppimaan jo aiemmin tunnistetuista korvaustapauksista (Alpaydin, 2021). Väitettä tukee myös kansainväliset raportit, esimerkiksi EIOPA (2021) korostaa raportissaan, että kehittyneet analytiikkamenetelmät voivat merkittävästi parantaa petosten tunnistamisen tehokkuutta ja samalla minimoida väärin positiivisten määrää.

On tärkeää ottaa huomioon, että petosten tunnistamiseen ei ole käytössä yhtä ainoaa optimaalista menetelmää, vaan koneoppimismalleja käytetään usein rinnakkain toistensa tukena. Esimerkiksi valvotut menetelmät toimivat hyvin sellaisissa tilanteissa, jossa käytettävissä on laajasti tapaustilastoja, joilla tekoälyä voidaan kouluttaa. Valvomattomat menetelmät ovat vahvoja sellaisissa tilanteissa, joissa pyritään havaitsemaan uusia ja tuntemattomia petosmuotoja, sillä ne havaitsevat anomaliaita paremmin. (Hastie, Tibshirani & Friedman, 2009; Alpaydin, 2021) Vastaavasti puoliohjattu oppiminen soveltuu vakuutusalaan, sillä todettuja petostapauksia on vähän ja luokittelematonta dataa paljon (Zhu & Goldberg, 2009). Vahvistusoppiminen puolestaan voi tukea petosten torjuntaa hyödyntämällä prosessia, jossa järjestelmä oppii palkkioiden ja rangaistusten kautta parantamaan toimintaansa (Sutton & Barto, 2018).

Seuraavaksi tarkastellaan keskeisiä koneoppimismenetelmiä, joita on hyödynnetty vakuutuspetosten tunnistamisessa. Näihin kuuluu muun muassa päätöspuumallit, neuroverkot ja syväoppiminen, sekä erilaiset anomaliatunnistuksen menetelmät. Jokaisella menetelmällä on erilaiset vahvuudet ja rajoitteet, jotka vaikuttavat siihen millaisia petostapauksia niillä on optimaalista tutkia.

3.3 Keskeiset koneoppimismenetelmät vakuutuspetosten tunnistamisessa

Vakuutuspetosten tunnistamiseen on sovellettu useita koneoppimismenetelmiä ja tutkimusten perusteella esimerkiksi päätöspuut, tukivektorikoneet, neuroverkot, sekä valvomattomat menetelmät ovat osoittautuneet hyödyllisiksi. Päätöspuut ja niiden erilaiset laajennukset ovat olleet suosittu menetelmä, koska niitä on helppo tulkita. Päätöspuut ovat yksinkertaisia malleja, joissa päätökset tehdään haarautuvien ”oksien” avulla esimerkiksi

“jos–niin”-periaatteella. Päätöspohjaisia menetelmiä on jalostettu niin sanottuihin ensemble-muotoihin, jossa käytetään samaan aikaan useita päätöspuita, ja näistä tunnetuimpia ovat *Random Forest* ja *Gradient Boosting*. Erityisesti Gradient Boostingin optimoitu toteutus XGBoost on saavuttanut laajaa suosiota sen tehokkuudesta petosten tunnistamisessa (Chen & Guestrin, 2016). On kuitenkin tärkeää huomioida, että menetelmäkehitys on edennyt nopeasti 2010-luvun jälkeen, ja nykyiset tekoälymallit, kuten neuroverkot ja transformer-pohjaiset järjestelmät tarjoavat jo huomattavasti kehittyneempiä vaihtoehtoja erityisesti suurten ja monimuotoisten datamassojen analysointiin. Tästä huolimatta XGBoost on edelleen relevantti ja laajasti käytetty menetelmä vakuutuspetosten havaitsemisen tutkimuksessa ja käytännön sovelluksissa.

Tukivektorikoneet (SVM) ovat näytelleet keskeistä roolia monissa tutkimuksissa, sillä niillä on helppo soveltaa monimutkaisiakin rajapintoja. Tukivektorikone (SVM) on luokittelualgoritmi, jonka tavoitteena on löytää hypertaso, joka erottaa eri luokkien datapisteet mahdollisimman selkeästi toisistaan, ja näin ollen pystyy erottamaan petokset muusta datasta (EITCA Academy, n.d.). SVM on yksi suosituimmista menetelmistä vakuutuspetosten tunnistamisessa (Phua, Lee, Smith & Gayler, 2010).

Neuroverkot puolestaan jäljittelevät ihmisaivojen toimintaa yhdistämällä useita solmuja (neuroneja), ja ne kykenevät havaitsemaan tehokkaasti erilaisia riippuvuuksia analysoitavassa datassa. Näin ollen neuroverkot tarjoavat mahdollisuuden mallintaa monimutkaisia ja ei-lineaaraisia suhteita. Viaene, Dedene ja Derrig (2005) hyödynsivät Bayesilaisia neuroverkkoja auto-onnettomuuksiin liittyvien vakuutuspetosten tunnistamisessa ja osoittivat niiden tehokkuuden verrattuna perinteisiin menetelmiin.

Myös valvomattomat menetelmät ovat olleet suosittuja vakuutuspetosten tunnistamisessa. Valvomattomilla menetelmillä on suuri rooli erityisesti uusien petosmuotojen tunnistamisessa. Esimerkiksi Brockett, Derrig, Golden, Levine ja Alpert (2002) testasivat tutkimuksessaan pääkomponenttianalyysiä (PCA) ja RIDIT-menetelmää siten, että RIDIT kategorisoi vakuutusdatan erilaisiksi piirteiksi, jonka jälkeen PCA tiivistä nämä piirteet erilaisiksi pääkomponenteiksi. Lopulta, pääkomponentit jaoteltiin logistisella regressiolla, joka mahdollisti vakuutuspetosten tunnistamisen ilman ennalta merkittäviä esimerkkitapauksia.

3.4 Koneoppimismenetelmiin liittyvät haasteet ja rajoitteet

Vaikka koneoppimismenetelmät tarjoavat lupaavia mahdollisuuksia terveysvakuutuspetosten tunnistamiseen, niiden käyttöön liittyy sekä teknisiä, menetelmällisiä että eettisiä haasteita. Haasteet eivät koske ainoastaan mallien suorituskkyä, vaan myös sitä, miten tuloksia voidaan tulkita ja hyödyntää käytännön päätöksenteossa. Koneoppiminen toimii osana laajempaa vakuutusprosessia, jossa päätöksillä voi olla suoria vaikutuksia vakuutettujen oikeuksiin ja taloudelliseen hyvinvointiin. Tästä syystä haasteet voidaan jäsentää kahteen kokonaisuuteen: (1) teknisiin ja menetelmällisiin rajoitteisiin, jotka koskevat mallien toimivuutta ja datan käyttöä, sekä (2) eettisiin ja yhteiskunnallisiin haasteisiin, jotka liittyvät mallien oikeudenmukaisuuteen, läpinäkyvyyteen ja luottamukseen.

3.4.1 Teknisiin ja menetelmällisiin ratkaisuihin liittyvät haasteet ja rajoitteet

Vaikka koneoppimismenetelmät tarjoavat lupaavia ratkaisuja terveysvakuutuspetosten tunnistamiseen, niiden käyttöön liittyy merkittäviä teknisiä ja menetelmällisiä haasteita. Ensimmäinen keskeinen haaste on luokkien epätasapaino. Suurin osa vakuutuskorvaushakemuksista on laillisia, kun taas petostapauksia esiintyy harvoin, mikä johtaa siihen, että mallit oppivat luonnostaan tunnistamaan paremmin enemmistöluokan ja jättävät vähemmistöluokan eli petokset huomattavasti tunnistettaviksi. (He & Garcia, 2009)

Toinen haaste liittyy mallien läpinäkyvyyteen. Erityisesti syväoppimiseen perustuvat mallit toimivat usein ”musta laatikko” -periaatteella, jossa mallin päätöksentekoprosessia on vaikea selittää (Doshi-Velez & Kim, 2017). Terveysvakuutusjärjestelmässä tämä on ongelmallista, sillä vakuutusyhtiöillä on lainsäädännöllinen velvollisuus perustella asiakkaalle, miksi hänen hakemuksensa on hylätty tai merkitty epäilyttäväksi. Esimerkiksi EU:n tietosuojasetuksen (GDPR) artikla 22 antaa asiakkaalle oikeuden saada ymmärrettävä selitys automatisoiduista päätöksistä (Euroopan parlamentti ja neuvosto, 2016), mikä korostaa mallien selitettävyyden merkitystä.

Lisäksi koneoppimismallit ovat alttiita yli- ja alioppimiselle. Ylioppiminen tarkoittaa, että malli on oppinut liiaksi koulutusdatan yksityiskohtia ja menettää kykynsä yleistää uusiin tilanteisiin, kun taas alioppiminen merkitsee, ettei malli kykene havaitsemaan datan

olennaisia piirteitä (Bishop, 2006). Samalla petosten tekijät sopeuttavat toimintaansa mallien havaitsemistapoihin, mikä johtaa jatkuvaan "ratkaisu–vastaratkaisu" -dynamiikkaan. Tämä tekee petosten havaitsemisesta luonteeltaan dynaamisen prosessin, joka edellyttää mallien jatkuvaa päivytystä.

3.4.2 Eettiset ja yhteiskunnalliset haasteet ja rajoitteet

Koneoppimisen käyttö terveystakuutuspetosten havaitsemisessa ei liity pelkästään digitalisaation luomien mahdollisuuksien hyödyntämiseen, sillä siihen liittyy huomattavia eettisiä ja yhteiskunnallisia kysymyksiä. Ensimmäinen haaste liittyy päätöksenteon oikeudenmukaisuuteen. Jos koulutusdata sisältää piileviä rakenteellisia vinoumia, koneoppimismallit voivat vahvistaa tai tuottaa päätöksiä, jotka asettavat tietyt asiakasryhmät eriarvoiseen asemaan. (Barocas, Hardt & Narayanan, 2019) Tämä voi johtaa tilanteeseen, jossa petosepäilyt kohdistuvat systemaattisesti esimerkiksi tiettyihin sosioekonomisiin ryhmiin.

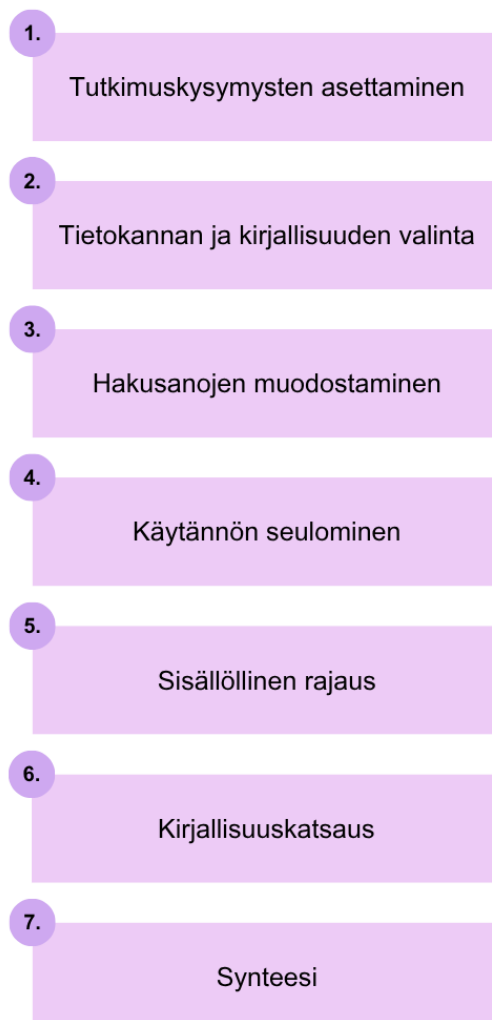
Toinen merkittävä haaste on luottamus. Vakuutusyhtiöiden päätöksillä on usein välittömiä vaikutuksia ihmisten terveyteen ja taloudelliseen turvallisuuteen. Sen vuoksi järjestelmän on oltava paitsi toimiva myös koettu oikeudenmukaiseksi. Mikäli asiakkaat kokevat koneoppimiseen perustuvat päätökset mielivaltaisiksi tai epäselviksi, seurauksena voi olla luottamuksen heikkeneminen koko vakuutusjärjestelmää kohtaan. (Doshi-Velez, F., & Been, K., 2017)

Lisäksi koneoppimiseen liittyvä energiankulutus ja ympäristövaikutukset ovat kasvava huolenaihe. Suurten mallien kouluttaminen vaatii huomattavaa laskentatehoa ja energiaa, mikä lisää kustannuksia ja herättää ympäristöetiikkaa koskevia kysymyksiä (Strubell, Ganesh & McCallum, 2019). Strubell ym. (2019) arvioivat, että pelkästään yhden syväoppimismallin kehitys-, optimointi- ja koulutusprosessi vastaa noin viiden henkilöauton koko elinkaaren hiilidioksidipäästöjä. Tämä havainnollistaa, että erityisesti terveydenhuollon kontekstissa, jossa resurssien tulisi kohdistua suoraan potilaiden hoitoon, suurten mallien käyttäminen voi olla vaikeasti perusteltavissa ilman merkittävää energiatehokkuutta tai laskennan optimointia.

4 KONEOPPIMISEN ROOLI TERVEYSVAKUUTUSPETOSTEN TUNNISTAMISESSA

4.1 Tutkimusaineiston hankinta ja esittely

Tutkimuksen empiirinen osuus toteutetaan systemaattisena kirjallisuuskatsauksena. Tämä alaluku käsittelee kirjallisuuskatsauksen tekoprosessia ja tutkimusaineiston hankintaa. Kirjallisuuskatsaus toteutettiin Finkin (2019, 6–7) seitsemävaiheisen mallin mukaisesti, jota kuvataan kuviossa 3.



Kuvio 3. Systemaattisen kirjallisuuskatsauksen vaiheet (muk. Fink, 2019)

Ensimmäisessä vaiheessa määritellään tutkimuskysymys, joka ohjaa katsauksen rakennetta ja rajausta. Tässä tutkielmassa keskeinen kysymys koskee sitä, miten koneoppimista voidaan hyödyntää terveystieteen tutkimusten tunnistamisessa. Toisessa vaiheessa valitaan kirjallisuuslähteet ja tietokannat, joista aineisto kerätään. Tämän tutkielman aineisto on kerätty hyödyntäen Tampereen yliopiston Andor-tietokantaa, joka mahdollistaa laajan pääsyn vertaisarvioituihin tieteellisiin julkaisuihin useista kansainvälisistä tietokannoista. Aineiston rajauksessa pyrittiin varmistamaan lähteiden korkea tieteellinen laatu, minkä vuoksi haku kohdistettiin ensisijaisesti vertaisarvioituihin artikkeleihin. Andor-tietokanta soveltui tähän tarkoitukseen erinomaisesti, sillä se tarjoaa luotettavan väylän korkeatasoisen tutkimuskirjallisuuden tavoittamiseen.

Kolmannessa vaiheessa valittiin hakutermit, jotka määrittävät millaisia julkaisuja analyysiin sisällytetään. Hakustrategian määrittelyssä käytettiin useita toisiaan täydentäviä hakusanoja, jotka yhdistettiin loogisilla operaattoreilla AND ja OR. Hakusanoilla pyrittiin tavoittamaan tutkimukset, joissa käsitellään koneoppimisen soveltamista terveystieteen tutkimuksessa. Taulukossa 1 on esitetty käytetyt hakusanat sekä muodostettu hakulauseke, jota sovellettiin hakuihin Andor-tietokannassa ja sen kattamissa alustoissa.

Hakusanat	Hakulauseke
health, medical, fraud, fraudulent, insurance, machine learning	(health OR medical) AND (fraud OR fraudulent) AND insurance AND machine learning

Taulukko 1

Tätä hakulauseketta käyttäen Tampereen yliopiston Andor-tietokannasta löytyi aluksi yhteensä 576 hakutulosta. Tämän jälkeen toteutettiin Finkin (2019, 7) mallin mukaiset käytännön seulonnat, joiden tavoitteena oli rajata tutkimuksen kannalta epärelevantit julkaisut pois ja kohdentaa haku tarkemmin itse tutkimuskysymyksiin. Käytännön seuloiksi

asetettiin vertaisarviointi, julkaisuvuodet 2020–2025 sekä englanninkielisyys. Näiden rajausten jälkeen hakutulosten määrä laski 117 artikkeliin.

Tämän jälkeen toteutettiin otsikkotason seulonta, jonka tarkoituksena oli poistaa tutkimukset, joiden otsikosta oli selvästi pääteltävissä, etteivät ne liittyneet terveysvakuutuksiin tai koneoppimiseen. Tässä vaiheessa karsittiin pois artikkelit, jotka käsittelivät esimerkiksi yleistä kyberturvallisuutta, muihin vakuutuslajeihin liittyviä petoksia tai muita vakuutusalaan irrallisia aiheita. Myös monimutkaiset määrälliset artikkelit pyrittiin rajaamaan pois, jotta laadullisen tutkimuksen punainen lanka säilyy. Otsikkotason seulonnan jälkeen aineistosta jäi jäljelle 23 artikkelia, jotka siirrettiin sisällöllisen arvioinnin vaiheeseen.

Seuraavassa vaiheessa suoritettiin metodologinen seulonta, jossa tarkasteltiin jäljelle jääneiden artikkelien tieteellistä laatua ja menetelmällistä luotettavuutta. Tässä vaiheessa analysoitiin, oliko tutkimuksissa käytetty menetelmä (esimerkiksi valvottu, valvomaton tai syväoppiminen) perusteltu tutkimusongelman ratkaisemiseksi, ja kuinka hyvin tutkimuksen toteutus ja tulokset raportoitiin. Arvioinnissa kiinnitettiin huomiota esimerkiksi siihen, selittikö tutkimus, miksi valittu menetelmä sopi petosten tunnistamiseen, miten data oli käsitelty ja kuinka selkeästi mallien toiminta ja tulokset oli raportoitu. Lopulliseen aineistoon valittiin tutkimuksia, jotka olivat menetelmiltään luotettavia, vastasivat suoraan tutkimuskysymyksiin ja kuvasivat analyysinsä riittävän tarkasti, jotta niiden tuloksia voi pitää uskottavina.

Katsaukseen valittiin seitsemän vertaisarvioitua artikkelia, jotka yhdessä tarjoavat monipuolisen ja ajankohtaisen kuvan koneoppimisen hyödyntämisestä terveysvakuutuspetosten tunnistamisessa ja ennaltaehkäisyssä. Seitsemän artikkelia muodostaa kandidaatintutkielman laajuuteen nähden hallittavan, mutta riittävän syvän aineiston, jonka avulla voidaan tuottaa luotettava ja kattava analyysi tutkimusaiheesta. Edellä kuvaillut seulonnan vaiheet esitetään taulukossa 2.

Rajaustyyppi	Rajaus	Osumat
Tietokanta	Tampereen yliopiston Andor	
Hakulauseke	(health OR medical) AND (fraud OR fraudulent) AND insurance AND machine learning	576
Kirjallisuuden tyyppi Kieli Ajallinen rajaus	Vertaisarvioitu englanti 2020–2025	117
Sisällöllinen rajaus	Soveltuvuus otsikko- ja tiivistelmätasolla	23
Lopullinen rajaus	Soveltuvuus tutkimuskysymysten kannalta	7

Taulukko 2

Taulukossa 3 esitetään kirjallisuuskatsaukseen valitut seitsemän vertaisarvioitua artikkelia, jotka muodostavat tutkimuksen empiirisen aineiston. Taulukko kokoaa yhteen kunkin artikkelin keskeiset tunnistetiedot (tekijät, otsikko, julkaisukanava ja julkaisuvuosi). Lisäksi taulukko sisältää artikkeleiden tunnistenumerot, joiden avulla niihin viitataan seuraavissa alaluvuissa.

Tunniste	Tekijä	Otsikko	Julkaisukanava	Vuosi
1	Cherkaoui, O., Anoun, H. & Maizate, A.	A benchmark of health insurance fraud detection using machine learning techniques	IAES	2024
2	De Meulemeester, H., De Smet, F., van Dorst, J., Derroitte, E. & De Moor, B.	Explainable unsupervised anomaly detection for healthcare insurance data	BMC Medical Informatics and Decision Making	2025
3	du Preez, A., Bhattacharya, S., Beling, P. & Bowen, E.	Fraud detection in healthcare claims using machine learning: A systematic review	Artificial Intelligence in Medicine	2025

4	Hancock, J.T. & Khoshgoftaar, T.M.	Gradient boosted decision tree algorithms for Medicare fraud detection	SN Computer Science	2021
5	Hancock, J.T., Bauder, R.A., Wang, H. & Khoshgoftaar, T.M.	Explainable machine learning models for Medicare fraud detection	Journal of Big Data	2023
6	Nabrawi, E. & Alanazi, A.	Fraud detection in healthcare insurance claims using machine learning	Risks	2023
7	Parthasarathy, S., Lakshminarayanan, A.R., Khan, A.A.A., Sathick, K.J. & Jayaraman, V.	Detection of health insurance fraud using Bayesian optimized XGBoost	International Journal of Safety and Security Engineering	2023

Taulukko 3

4.2 Tutkimusaineiston analyysi

Finkin (2019, 7) esittämän systemaattisen kirjallisuuskatsauksen mallin viimeinen vaihe on valitun aineiston synteessin tuottaminen. Tässä tutkimuksessa synteesi toteutettiin aineistolähtöisen sisällönanalyysin avulla. Aineistolähtöisen sisällönanalyysin tarkoituksena on tiivistää ja jäsentää laaja aineisto siten, että sen olennainen merkityssisältö tulee näkyväksi (Tuomi & Sarajärvi, 2018, 90–91). Menetelmä soveltuu tähän tutkimukseen, sillä analyysin tavoitteena ei ole testata ennalta määriteltyä hypoteesia, vaan tunnistaa toistuvia rakenteita ja merkityssuhteita tutkimuksissa, joissa käsitellään koneoppimismenetelmien hyödyntämistä terveystakuutuspetosten tunnistamisessa.

Aineistolähtöinen sisällönanalyysi eteni kolmivaiheisesti: pelkistäminen, ryhmittely ja käsitteellistäminen (Miles & Huberman, 1994, 10; Tuomi & Sarajärvi, 2018, 91–93). Ensimmäisessä vaiheessa analysoiduista artikkeleista kerättiin tutkimuskysymysten kannalta keskeiset sisällöt, jotka tiivistettiin pelkistetyiksi ilmaisuiksi. Ensimmäisen tutkimuskysymyksen kohdalla tarkasteltiin kuvauksia siitä, millainen rooli koneoppimismenetelmillä on terveystakuutuspetosten tunnistamisessa. Toisen

tutkimuskysymyksen kohdalla kerättiin ilmaukset muuttujista ja tietolähteistä, joita mallit hyödyntävät petosepäilyjen arvioinnissa. Taulukossa 4 esitetään esimerkki pelkistämispöytäkirjasta.

Tunniste	Alkuperäinen ilmaus	Pelkistetty ilmaus
2	“The proposed workflow is able to detect known care providers with atypical behaviour and helps expert investigators in making informed decisions.”	Poikkeava palveluntarjoajakäyttäytyminen

Taulukko 4

Toisessa vaiheessa, ryhmittelyssä samankaltaiset pelkistetyt ilmaisut koottiin alaluokkiin (Tuomi & Sarajärvi, 2018, 92). Koneoppimisen käyttötarkoitusta kuvaavat ilmaisut ryhmittyivät ensin esimerkiksi valvottuun ja valvomattomaan oppimiseen, jonka jälkeen ilmaisut jaoteltiin näiden ryhmien sisällä esimerkiksi anomaliatunnistuksen, luokittelupohjaisen tunnistamisen ja riskipisteytysmallien alaluokkiin. Petosten tunnistamisessa käytetyt muuttujat puolestaan ryhmittyivät esimerkiksi korvaustapahtumiin liittyviin tietoihin (esim. laskutuksen sisältö ja määrä), palveluntarjoajaan liittyviin tietoihin (esim. ammattiprofiili, hoitokäytännöt) sekä hoitoketjua kuvaaviin tietoihin (esim. diagnoosin ja toteutetun hoidon vastaavuus). Ryhmittelystä esitettyä esimerkkiä kuvataan taulukossa 5.

Alaluokka	Pelkistykset
Korvaustapahtumiin liittyvät tiedot	Laskutuksen sisältö Laskutuksen määrä Laskutuksen toistuvuus

Taulukko 5

Viimeisessä vaiheessa alaluokat koottiin kahdeksi pääluokaksi, jotka muodostavat tämän tutkielman analyysilukujen rakenteen. Ensimmäinen pääluokka kuvaa koneoppimismenetelmien roolia terveystakuutuspetosten tunnistamisessa, ja toinen pääluokka tarkastelee menetelmissä hyödynnettyjä tietolähteitä ja muuttujia. Käsitteellistämässä huomioitiin myös agenttiteorian näkökulma, sillä osa tunnistettavista muuttujista (esim. epätavalliset laskutusprofiilit tai toistuvat palveluntarjoajakuvioinnit) kytkeytyy moraalikadon ja haitallisen valikoitumisen mekanismeihin. Analyysiprosessi mahdollisti sekä tutkimuskysymysten systemaattisen tarkastelun että terveystakuutuspetosten ilmiön rakenteellisen ymmärtämisen. Näiden havaintojen synteesi esitetään seuraavissa alaluvuissa (4.3 ja 4.4).

Yhteenvedon analyysistä voidaan todeta, että aineiston tutkimukset olivat pääosin samansuuntaisia menetelmien tehokkuuden ja käytettyjen muuttujien suhteen. Merkittäviä keskinäisiä ristiriitoja ei havaittu, mikä on itsessään huomionarvoinen tulos. Tämä konsensus viittaa siihen, että terveystakuutuspetosten tunnistamiseen käytettävät koneoppimismenetelmät ovat kehittyneet erilaisissa tutkimusympäristöissä samankaltaiseen suuntaan. Pienet erot liittyivät lähinnä siihen, millaisissa olosuhteissa valvotut, valvomattomat tai hybridimallit suoriutuivat parhaiten, mutta nämä erot heijastivat enemmän aineistojen ja tutkimusasetelmien erilaisuutta kuin varsinaisia teoreettisia ristiriitoja.

4.3 Koneoppimismenetelmien hyödyntäminen terveystakuutuspetosten tunnistamisessa

Seuraavat havainnot perustuvat aineistolähtöiseen sisällönanalyysiin, jossa tutkimusaineistoa tarkasteltiin erityisesti palveluntarjoajien toimintaprofiilien, laskutuskäyttäytymisen ja hoitoketjujen rakenteiden näkökulmasta. Tavoitteena oli tunnistaa, millaisia lainalaisuuksia eri tutkimuksissa toistuu riippumatta käytetystä maantieteellisestä kontekstista, datarakenteesta tai mallinnustavasta.

Terveystakuutuspetosten keskeisenä haasteena on, että ne naamioituvat osaksi tavanomaisia korvaus- ja hoitoprosesseja. Petos ei useinkaan ilmene yksittäisenä poikkeavana korvaushakemuksena, vaan se rakentuu vähitellen näkyviksi tulevista laskutusrutiineista, hoitoketjuista ja toimintamalleista [2; 3; 5]. Tämän vuoksi

sääntöpohjaiset valvontajärjestelmät, jotka perustuvat valmiiksi määriteltyihin hälytysehtoihin, jäävät helposti jälkeen tilanteissa, joissa toimintamallit muuttuvat, mutta yksittäinen tapahtuma ei näytä epäilyttävältä [3; 6].

Aineiston mukaan petos on useammin palveluntarjoajalähtöistä kuin yksittäisten asiakkaiden toteuttamaa [3; 6]. Palveluntarjoaja voi esimerkiksi laskuttaa toimenpiteitä, joita ei voida perustella diagnoosilla, kasvattaa toimenpidevolyymeja ilman lääketieteellistä syytä tai suunnitella hoitopolkuja, jotka ovat näennäisesti hyväksyttäviä mutta taloudellisesti optimointiin perustuvia [6; 7]. Näissä tapauksissa koneoppimisen roolina on tunnistaa poikkeavia käyttäytymisprofiileja, joissa toiminta eroaa samassa toimintaympäristössä toimivien muiden palveluntarjoajien käyttäytymisestä.

Koneoppimisen vahvuus on sen kyky tarkastella pitkäaikaista käyttäytymistä, ei vain yksittäisiä tapahtumia. Normaali laskutusikäyttäytyminen on yleensä suhteellisen pysyvää, sillä toimijoilla on tunnistettava hoitotyyli, potilasjakauma ja kustannusrakenne. Petollisen toiminnan yhteydessä nämä rakenteet alkavat muuttua tavalla, joka poikkeaa historiallisesta ja vertailuryhmistä. [2; 3; 5] Siksi mallien tulee käsitellä tietoa aikasarjoina ja profiileina, ei vain pistehavaintoina.

Aineistossa korostuu, että koneoppiminen mahdollistaa valvonnan ennakoivan kohdistamisen. Mallien tuottamien riskipisteiden avulla tarkastuksia voidaan suunnata niihin toimijoihin, joissa petoksen riski on kohonnut [3; 4; 7]. Tämä tehostaa valvontaa, sillä laajat manuaaliset tarkastukset ovat hitaita ja kalliita. Koneoppiminen ei kuitenkaan korvaa asiantuntijatyötä, vaan toimii seulana, joka nostaa esiin tapaukset tarkempaa tutkimusta varten [1; 3].

Vaikka koneoppiminen tarjoaa merkittäviä mahdollisuuksia, aineistossa korostuu myös sen käyttöön liittyviä haasteita. Ensimmäinen haaste on epätasapainoinen aineisto. Petostapauksia on tyypillisesti vain murto-osa kaikista korvaustapahtumista, mikä voi johtaa siihen, että mallit oppivat tunnistamaan kaiken normaaliksi, ellei aineistoa käsitellä tarkoituksenmukaisesti [3; 5; 6]. Tämän ratkaisemiseen käytetään esimerkiksi näytteenoton tasapainotusta tai sopivia mallivalintoja, mutta valinnat vaikuttavat suoraan mallien luotettavuuteen.

Toinen keskeinen haaste liittyy datan laatuun ja kattavuuteen. Jos palveluntarjoajien hoitoprofiilit tai korvaushistoriat ovat puutteellisia tai eri järjestelmistä koottuja, mallien kyky oppia käyttäytymisrakenteita heikkenee [2; 3; 6]. Tämä voi johtaa joko ali- tai ylioppimiseen. Kolmas toistuva haaste on tulkittavuus. Malli voi tunnistaa poikkeaman, mutta ilman selkeää selitystä vaarana on, että valvonta ei voi perustella jatkotoimia hallinnollisesti tai oikeudellisesti [1; 4]. Tämän vuoksi mallien käyttöönotto vaatii mekanismeja, joiden avulla voidaan selittää, miksi jokin toimija poikkeaa odotetusta.

Koneoppiminen tunnistaa terveystakuutuspetoksia tarkastelemalla toiminnan rakenteita ja muutoksia ajan kuluessa, mikä mahdollistaa valvonnan siirtämisen reaktiivisista tarkastuksista ennakoivaan ja riskiperusteiseen ohjaukseen. Jotta tätä voidaan hyödyntää luotettavasti, mallien kehittäminen edellyttää epätasapainoisen aineiston käsittelyä, riittävän kattavaa ja laadukasta dataa sekä mallien tulosten tulkittavuutta, jotta niitä voidaan käyttää hallinnollisesti ja oikeudellisesti kestävästi. Näiden edellytysten täytyessä koneoppiminen tarjoaa välineen, joka ei korvaa asiantuntijaa, mutta vahvistaa ja kohdentaa valvontatyötä, mikä on keskeistä terveystakuutusjärjestelmän väärinkäytösten ennaltaehkäisyssä.

4.4 Koneoppimismenetelmien käytössä hyödynnetyt menetelmät ja muuttujat

Tässä alaluvussa esitettävät tulokset muodostuivat analyysin ryhmittelyvaiheessa, jossa eri tutkimuksissa kuvatut koneoppimismenetelmät sekä niissä käytetyt tietotyypit koottiin laajemmiksi käsitteellisiksi kokonaisuuksiksi. Tarkastelun kohteena ei ollut yksittäisten mallien tekninen suorituskyky, vaan menetelmien rooli petoksen tunnistamisen prosessissa ja niiden hyödyntämä tietopohja.

Aineiston perusteella ei ole olemassa yhtä selvästi parasta koneoppimismenetelmää terveystakuutuspetosten tunnistamiseen, vaan menetelmävalinta riippuu siitä, millaista dataa on saatavilla ja mikä on valvonnan tavoite [3; 6; 7]. Kuitenkin useissa tutkimuksissa toistuu havainto siitä, että päätöspuupohjaiset menetelmät, kuten Random Forest sekä erilaiset gradienttivahvistetut mallit (esim. XGBoost, LightGBM, CatBoost), ovat käytännön valvonnassa erityisen käyttökelpoisia [3; 4; 5; 7]. Niiden etuna on kyky käsitellä samanaikaisesti suuri määrä muuttujia ilman, että tietoa tarvitsee muokata kapeisiin, ennalta yhtenäistettyihin muotoihin. Tämä on tärkeää terveystakuutusjärjestelmissä, joissa tieto on

usein sekä numeerista (kustannukset ja määrät), että luokittelevia koodeja (diagnoosit, toimenpiteet).

Päätöspuupohjaisten mallien käytännön vahvuus on myös se, että ne kykenevät huomioimaan muuttujien väliset suhteet. Tämä on olennaista petostapauksissa, jotka eivät näy yksittäisinä poikkeamina, vaan käyttäytymisen rakenteellisina kuvioina. Esimerkiksi palveluntarjoaja voi laskuttaa tiettyä toimenpidettä täysin hyväksyttävissä määrissä, mutta jos kyseinen toimenpide esiintyy erittäin usein tietyn diagnoosin kanssa, jota tavallisesti ei hoideta tällä toimenpiteellä, muodostuu mallille riskisignaali [3; 6]. Tällaiset suhteet eivät ole yksiselitteisesti koodattavissa sääntöihin, mutta koneoppiminen kykenee havaitsemaan ne.

Aineistossa esiintyy myös valvomattomien menetelmien käyttö, erityisesti tilanteissa, joissa petostapauksia ei ole merkitty luotettavasti tai niitä on vähän suhteessa kokonaisdataan [2; 6]. Valvomattomat menetelmät etsivät poikkeuksellisia toimintamalleja, kuten poikkeuksellisen suuria toimenpidemääriä, epätavallisia hoitopolkuja tai kustannusrakenteita, jotka eivät sovi muiden tuottajien profiiliin. Näitä menetelmiä hyödynnetään usein alustavana seulontakerroksena, jonka jälkeen asiantuntijat tai valvotut mallit tarkentavat arviota [1; 3].

Aineistossa toistuu vahva johtopäätös siitä, että käytännössä paras tulos saavutetaan yhdistämällä valvottuja ja valvomattomia menetelmiä. Tätä kutsutaan hybridimalliksi. Hybridimallissa valvomaton mallinnus tunnistaa palveluntarjoajaprofiileja, jotka poikkeavat merkittävästi vertailuryhmästä ja valvottu luokittelija puolestaan arvioi poikkeamien petostodennäköisyyden käyttäen historiallisesti varmistettuja petostapauksia opetusmateriaalina [2; 3; 4; 6; 7]. Hybridimalli on tehokas erityisesti siksi, että valvottu luokittelu tarvitsee opetusaineiston, mutta opetusaineisto on harvoin kattava. Valvomaton analyysi laajentaa näkyvyyttä, valvottu analyysi syventää tulkintaa.

Aineiston perusteella terveystakuutuspetosten tunnistamisessa käytettyjä muuttujia voidaan jäsentää kolmen toisiaan täydentävän näkökulman mukaan. Ensimmäinen näkökulma liittyy toimenpiteisiin ja kustannuksiin: mitä laskutetaan, kuinka usein ja millä hinnalla. Tällä tasolla koneoppiminen kykenee paljastamaan esimerkiksi yllaskutusta tai taloudellisesti kannattaviin toimenpiteisiin perustuvaa laskutusrakenteen manipulointia [3; 6; 7]. Toinen näkökulma koskee palveluntarjoajan profiilia, johon sisältyvät esimerkiksi

erikoisala, sijainti, resurssit ja potilasjakauma. Näiden avulla voidaan vertailla, onko toiminta linjassa muiden samankaltaisessa asemassa toimivien palveluntuottajien kanssa [2; 3; 7]. Kolmas näkökulma on hoitoketjun johdonmukaisuus: vastaako käytetty hoito diagnoosia, ja eteneekö hoitoprosessi lääketieteellisesti perustellulla tavalla. Tämän avulla voidaan tunnistaa esimerkiksi keinotekoisia tai perusteettomia hoitopolkuja [6; 7].

Käytännön esimerkki havainnollistaa muuttujien yhteisvaikutusta. Yksittäinen fysioterapiakäynti ei ole itsessään epäilyttävä. Sen sijaan riskiprofiili muodostuu silloin, kun palveluntarjoaja laskuttaa fysioterapiaa poikkeuksellisen paljon verrattuna muihin vastaavan erikoisalan toimijoihin, tekee sen diagnooseilla, joita harvoin hoidetaan fysioterapialla, ja jatkaa samaa hoitoa ilman potilaan tilan muutoksia. Tällöin ei ole kyse yksittäisestä kustannuspoikkeamasta, vaan toimintamallista, joka eroaa systemaattisesti vertailuryhmien käytännöistä [3; 6]. Näin ollen koneoppimisen tuottama riskimerkki syntyy muuttujien yhdistelmästä, ei yksittäisestä arvosta.

Yhteenvetona voidaan todeta, että petosten tunnistamisessa puupohjaiset mallit ovat käyttökelpoisia tilanteissa, joissa muuttujien väliset suhteet ovat keskeisiä ja korvausdata monimutkaista [3; 4; 5; 7]. Valvomattomat menetelmät puolestaan mahdollistavat epätyypillisten tapausten havaitsemisen silloin, kun petostapauksia ei ole merkitty riittävästi tai ne ovat luonteeltaan muuttuvia [2; 6]. Paras tulos saavutetaan mallien yhdistelmällä, jossa valvoton analyysi toimii seulontakerroksena ja valvottu analyysi tarkentavana luokitteluvaiheena [1; 3]. Lopulta olennaista on kuitenkin se, että riskisignaali muodostuu toiminnan rakenteesta ja sen muutoksista, ei yksittäisestä epäilyttävästä tapahtumasta [3; 6; 7].

5 JOHTOPÄÄTÖKSET

5.1 Keskeiset tulokset

Tutkimuksen tavoitteena oli vastata kahteen tutkimuskysymykseen:

1. Miten koneoppimismenetelmiä voidaan hyödyntää terveystakuutuspetosten tunnistamisessa ja ennaltaehkäisyssä?
2. Millaisia menetelmiä ja muuttujia koneoppimismallit hyödyntävät tunnistamisprosessissa?

Aineistolähtöinen sisällönanalyysi osoitti, että molemmat kysymykset kytkeytyvät olennaisesti terveystakuutuspetosten rakenteelliseen luonteeseen. Tätä havaintoa tukee myös aiempi tutkimus, jonka mukaan terveystakuutuspetokset eivät useimmiten ilmene yksittäisinä väärin perustein tehtyinä korvausvaatimuksina, vaan ne rakentuvat vähitellen muodostuvista toimintamalleista, laskutusrutiineista ja hoitoketjujen epäjohdonmukaisuuksista (Viaene & Dedene, 2004; Gee & Button, 2019). Samalla tulos on linjassa agenttiteorian ja epäsymmetrisen informaation näkökulmien kanssa, joiden mukaan vakuutusjärjestelmä altistuu moraalikadolle silloin, kun vakuutuksenottajan toimintaa on vaikea havaita tai valvoa (Rothschild & Stiglitz, 1976; Eisenhardt, 1989). Näin ollen aineiston havainnot vahvistavat teoreettisen lähtökohdan siitä, että petokset syntyvät usein tilanteissa, joissa toimijoiden välinen tieto ei ole tasapainoista.

Ensimmäisen tutkimuskysymyksen osalta keskeinen tulos on, että koneoppimismenetelmien hyödyntäminen perustuu niiden kykyyn tarkastella hoito- ja laskutusprosessien pitkäikäisyyttä. Aineiston tutkimuksissa mallit eivät arvioineet vain yksittäisiä tapahtumia, vaan ne tunnistivat, miten toiminta muuttuu ajan kuluessa suhteessa vertailuryhmiin. Tätä tukee myös aiempi tutkimus, jonka mukaan perinteiset sääntöpohjaiset järjestelmät eivät skaalaudu suurille datamäärille eivätkä kykene havaitsemaan uusia petosmuotoja (Bolton & Hand, 2002). Samansuuntaisia havaintoja esittävät Bauder et al. (2018), joiden mukaan hybridimallit havaitsevat tehokkaasti poikkeavia laskutusmalleja, sekä Phua et al. (2010), jotka korostavat, että petokset paljastuvat usein epätavallisista muuttujayhdistelmistä. Aineiston tulokset ovat siten selkeästi linjassa aiemman kirjallisuuden kanssa ja vahvistavat käsitystä siitä, että koneoppiminen soveltuu erityisesti

rakenteellisten petosmallien tunnistamiseen, eli juuri niihin tilanteisiin, joita agenttiteoria pitää moraalikadon kannalta riskialttiina.

Koneoppimisen tuottamat riskisignaalit toimivat käytännössä seulontamekanismina. Aineiston mukaan mallit eivät määritä suoraan, onko kyseessä petos, vaan ne tuottavat todennäköisyysarvioita tai poikkeamia, joiden perusteella asiantuntijat voivat kohdentaa tarkastuksiaan. Tätä havaintoa tukee myös Joudaki et al. (2015), joiden mukaan terveysvakuutuspetosten arviointi edellyttää aina asiantuntijan tulkintaa ja kontekstin ymmärrystä. Aineiston ja aiemman tutkimuksen perusteella koneoppimisen rooli on siten selvästi täydentävä, sillä se vahvistaa valvonnan tehokkuutta ja laajuutta ilman, että se korvaa asiantuntijan työtä tai oikeudellista vastuuta. Tämä on linjassa agenttiteorian kanssa, jonka mukaan valvontamekanismien vahvistaminen vähentää moraalikadon riskiä.

Toisen tutkimuskysymyksen osalta aineisto osoitti, että petosten tunnistaminen edellyttää moniulotteista tietopohjaa, joka kuvaa paitsi yksittäisiä korvaustapahtumia myös palveluntarjoajan toimintaympäristöä ja hoitoketjujen rakennetta. Tätä havaintoa tukee myös aiempi tutkimus, jonka mukaan terveysvakuutuspetokset ovat usein rakenteellisia ja edellyttävät laajaa kontekstuaalista tietoa (Gee & Button, 2019; Joudaki et al., 2015). Aineiston tulokset ovat linjassa myös sen kanssa, että petosten havaitseminen edellyttää useiden tietolähteiden yhdistämistä ja vertailua, kuten hoitoketjujen, laskutuksen ja diagnoosien välisten suhteiden tarkastelua. Näin ollen aineiston havainnot vahvistavat kirjallisuudessa esitetyn näkemyksen siitä, että petosten tunnistaminen edellyttää laajaa ja moniulotteista tietopohjaa, joka puolestaan on johdonmukaista agenttiteorian oletuksen kanssa siitä, että tiedon epäsymmetria on petosten keskeinen mahdollistaja.

Aineiston perusteella ei ole olemassa yhtä yleisesti parasta koneoppimismenetelmää. Päätöspuupohjaiset ensemble-mallit, kuten Random Forest ja XGBoost, suoriutuivat hyvin epätasapainoisissa aineistoissa, joissa petostapaukset ovat harvinaisia, kuten myös Bauder & Khoshgoftaar (2018) ovat todenneet. Valvomattomat menetelmät, kuten klusterointi, olivat puolestaan hyödyllisiä tilanteissa, joissa petosten esiintyvyys ei ollut luotettavasti merkattua, jota tukee myös aiempi tutkimus, ks. Phua et al., 2010. Aineiston ja aiemman kirjallisuuden perusteella parhaat tulokset saavutettiin hybridimalleilla, joissa poikkeavuuksien tunnistus ja valvottu luokittelu täydentävät toisiaan. Tämä havainto toistui useissa tutkimuksissa ja muodostaa selkeän konsensuksen.

Yhteenvedon voidaan todeta, että koneoppimisen vahvuus terveystieteen tunnistamisessa on sen kyky löytää poikkeavaa käyttäytymistä, joka ei välttämättä näy yksittäisissä korvaustapahtumissa, vaan muodostuu vähitellen toiminnan tasolla. Tätä havaintoa tukee sekä aiempi tutkimus että tämän tutkielman analyysi. Aineiston perusteella tutkimuskenttä oli yllättävän yhteneväinen, sillä merkittäviä ristiriitoja ei havaittu. Tämä on linjassa aiemman kirjallisuuden kanssa ja viittaa siihen, että menetelmät ja arviointikriteerit ovat kehittyneet samansuuntaisesti eri tutkimusympäristöissä. Näin ollen voidaan todeta, että koneoppiminen tarjoaa lupaavan ja jo osittain vakiintuneen välineen terveystieteen tunnistamiseen ja ennaltaehkäisyyn. Samalla se vastaa agenttiteorian esittämään tarpeeseen vahvistaa valvontaa ja vähentää tiedon epäsymmetriaa vakuutusjärjestelmässä.

5.2 Tutkimuksen arviointi ja jatkotutkimusehdotukset

Tutkimuksen vahvuutena on sen johdonmukaisesti toteutettu ja läpinäkyvä analyysiprosessi. Aineistolähtöinen sisällönanalyysi sopi tutkimuskysymyksiin hyvin, sillä tavoitteena ei ollut vertailla yksittäisten koneoppimismenetelmien teknistä suorituskäyttöä, vaan ymmärtää niiden roolia terveystieteen tunnistamisessa sekä sitä, millaisiin tietorakenteisiin tunnistus nojaa. Menetelmä mahdollisti sen, että eri tutkimuksista nousseita teemoja voitiin vertailla ja jäsentää osaksi laajempaa kokonaiskuvaa ilmiöstä. Näin tulokset kuvaavat ensisijaisesti tieteen tunnistamisen logiikkaa, eivät yksittäisiä mallien numeerisia suorituksia.

Tutkimuksella on kuitenkin myös rajoituksia. Merkittävin niistä liittyy siihen, ettei tässä työssä ollut käytettävissä suomalaista terveystieteen aineistoa. Analyysi perustuu kansainvälisiin tutkimuksiin, joiden toimintaympäristöt ja korvauskäytännöt voivat poiketa suomalaisesta järjestelmästä. Tämä ei tee tuloksista käyttökelvottomia, mutta se tarkoittaa, että menetelmien käytännön soveltaminen Suomessa edellyttää jatkotutkimusta. Toinen suuri haaste liittyy siihen, että suurin osa lähdeaineistosta oli hyvin teknistä. Koneoppimismalleja, parametrivalintoja ja erilaisia mittareita esiteltiin usein oletuksella, että lukija tuntee menetelmät ennestään. Tämä johti siihen, että keskeisiä käsitteitä ja mallien toimintaperiaatteita oli avattava erikseen, jotta niiden yhteys tieteen tunnistamiseen ja valvontaprosesseihin säilyi ymmärrettävänä. Tutkimusprosessin aikana kävi selväksi, että mallien tulkittavuus ja läpinäkyvyys ei ole ainoastaan käytännön valvontatyön vaatimus,

vaan myös tutkimuksen tekemisen edellytys, sillä jos mallia ei voi selittää, sen merkitys ilmiössä jää väkisininkin epäselväksi.

Tutkimuksen luotettavuutta voidaan tarkastella reliabiliteetin ja validiteetin näkökulmista. Reliabiliteetti tarkoittaa laadullisessa tutkimuksessa toistettavuutta. (Kirk & Miller, 1986) Tässä työssä reliabiliteettia vahvistettiin siten, että analyysin eteneminen dokumentoitiin vaiheittain, jolloin on mahdollista jäljittää, miten alkuperäisistä teksteistä päädyttiin muodostettuihin teemoihin. Näin ollen tutkimus on toistettavissa siinä laajuudessa, jossa kirjallisuuskatsauksen hakuprosessi, valintakriteerit ja analyysimenetelmä on kuvattu, ja ulkopuolinen tutkija voi niiden perusteella seurata samaa menettelyä. Lisäksi analyysiin pyrittiin sisällyttämään sellaisia havaintoja, jotka toistuivat useissa eri lähteissä. Yksittäisiä tai poikkeavia havaintoja puolestaan ei nostettu tulosten perustaksi.

Validiteetti tarkoittaa sitä, tutkiiko työ todella sitä ilmiötä, jota sen väitetään tutkivan (Kirk & Miller, 1986). Tässä tutkimuksessa validiteettia vahvistaa se, että analyysissa edettiin aineistolähtöisesti, sillä tulkinat muodostettiin tutkimusaineistosta käsin, eikä niitä johdettu valmiista oletuksista. Validiteettia rajoittaa kuitenkin se, että menetelmien käytännön toimivuutta ei arvioitu suomalaisessa valvontaympäristössä. Täten tulokset kuvaavat luotettavasti ilmiön rakennetta, mutta eivät vielä kerro, miten hyvin mallit toimivat käytännössä Suomessa.

Jatkossa olisi tärkeää toteuttaa tutkimus, jossa koneoppimismenetelmiä testataan suomalaisella terveystakuutusdatalla. Tällainen tutkimus näyttäisi käytännössä, kuinka hyödyllisiä mallit olisivat suomalaisen vakuutusalan tulevaisuudelle. Lisäksi olisi tarpeen kehittää menetelmiä, joiden avulla mallien tuottamat havainnot voidaan selittää selkeästi myös niille, jotka tekevät päätöksiä valvonnassa tai korvauskäsittelyssä. Tämä on tärkeää siksi, että koneoppimisen rooli ei voi perustua "mustaan laatikkoon", vaan sen tuottamat tulokset täytyy pystyä perustelemaan.

LÄHDELUETTELO

4.4 Kirjallisuuslähteet

- Alpaydin, E. (2020). Introduction to machine learning (Fourth edition.). The MIT Press.
- Arrow, K. J. (1963). Uncertainty and the Welfare Economics of Medical Care. *The American Economic Review*, 53(5), 941–973
- Barocas, S., Hardt, M., & Narayanan, A. (2019). *Fairness and machine learning*. fairmlbook.org. <https://fairmlbook.org>
- Bauder, R. A., & Khoshgoftaar, T. M. (2018). The detection of Medicare fraud using machine learning methods. *Proceedings of the Thirty-First International Florida Artificial Intelligence Research Society Conference*, 404. <https://cdn.aaai.org/ocs/17617/17617-77660-1-PB.pdf>
- Bishop, C. M. (2006). *Pattern recognition and machine learning*. Springer. <https://link.springer.com/book/10.1007/978-0-387-45528-0>
- Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, 17(3), 235–249. <https://doi.org/10.1214/ss/1042727940>
- Brockett, P. L., Derrig, R. A., Golden, L. L., Levine, A., & Alpert, M. (2002). Fraud Classification Using Principal Component Analysis of RIDITs. *The Journal of Risk and Insurance*, 69(3), 341–371. <https://doi.org/10.1111/1539-6975.00027>
- Button, M., & Gee, J. (2013). *Countering fraud for competitive advantage : the professional approach to reducing the last great hidden cost* (1st edition). Wiley.
- Button, M., Johnston, L., Frimpong, K., & Smith, G. (2007). New directions in policing fraud: The emergence of the counter fraud specialist in the United Kingdom. *International Journal of the Sociology of Law*, 35(4), 192–208. <https://doi.org/10.1016/j.ijsl.2007.06.002>
- CUMMINS, J. D., & TENNYSON, S. (1996). Moral Hazard in Insurance Claiming: Evidence from Automobile Insurance. *Journal of Risk and Uncertainty*, 12(1), 29–50. <https://doi.org/10.1007/BF00353329>
- Derrig, R. A. (2002). Insurance Fraud. *The Journal of Risk and Insurance*, 69(3), 271–287. <https://doi.org/10.1111/1539-6975.00026>
- Dionne, Georges. (Ed.). (2013). *Handbook of Insurance* (2nd ed. 2013.). Springer New York. <https://doi.org/10.1007/978-1-4614-0155-1>

- Dionne, G., Giuliano, F., & Picard, P. (2009). Optimal Auditing with Scoring: Theory and Application to Insurance Fraud. *Management Science*, 55(1), 58–70. <https://doi.org/10.1287/mnsc.1080.0905>
- Doshi-Velez, F., & Been, K. (2017). Towards A Rigorous Science of Interpretable Machine Learning. arXiv.Org.
- Eisenhardt, K. M. (1989). Agency Theory: An Assessment and Review. *The Academy of Management Review*, 14(1), 57–74. <https://doi.org/10.2307/258191>
- Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. The MIT Press.
- Hastie, T., Tibshirani, R., & Friedman, J. (2009). *The Elements of Statistical Learning : Data Mining, Inference, and Prediction, Second Edition (2nd ed. 2009.)*. Springer New York. <https://doi.org/10.1007/978-0-387-84858-7>
- Haibo He, & Garcia, E. A. (2009). Learning from Imbalanced Data. *IEEE Transactions on Knowledge and Data Engineering*, 21(9), Article 5128907. <https://doi.org/10.1109/TKDE.2008.239>
- J. Gee ja M. Button, *The financial cost of healthcare fraud 2015: What data from around the world shows*, London: Forensic & Counter Fraud Service, 2015.
- Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2015). Using data mining to detect health care fraud and abuse: A review of literature. *Global Journal of Health Science*, 7(1).
- Kirk, Y., & Miller, M. L. (1986). *Reliability and validity in qualitative research (1st ed., Vol. 1)*. Sage. <https://doi.org/10.4135/9781412985659>
- Mitchell, T. M. (1997). *Machine learning*. McGraw-Hill.
- Mossin, J. (1968). Aspects of Rational Insurance Purchasing. *The Journal of Political Economy*, 76(4), 553–568. <https://doi.org/10.1086/259427>
- Murphy, K. P. (2012). *Machine learning: A probabilistic perspective*. MIT Press.
- Outreville, J. F. (1998). *Theory and Practice of Insurance (1st ed.)*. Springer. <https://doi.org/10.1007/978-1-4615-6187-3>
- Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A Comprehensive Survey of Data Mining-based Fraud Detection Research. arXiv.Org. <https://doi.org/10.48550/arxiv.1009.6119>
- Picard, P. (2000). Economic Analysis of Insurance Fraud. In G. Dionne (Ed.), *Handbook of Insurance* (pp. 315–362). Springer Netherlands. https://doi.org/10.1007/978-94-010-0642-2_10

- Rantakangas, A. (2021). *Koneoppimisen tulevaisuus vakuutusyhtiöiden työvälineenä* [Pro gradu -tutkielma, Tampereen yliopisto]. Trepo.
<https://trepo.tuni.fi/bitstream/handle/10024/135837/RantakangasAliina.pdf>
- Rantala, J., & Kivisaari, E. & Ellibs. (2020). *Vakuutusoppi* (13. uudistettu painos). FINVA.
- Rothschild, M., & Stiglitz, J. (1976). Equilibrium in Competitive Insurance Markets: An Essay on the Economics of Imperfect Information. *The Quarterly Journal of Economics*, 90(4), 629–649. <https://doi.org/10.2307/1885326>
- Russell, S. J. (Stuart J., & Norvig, P. (2016). *Artificial intelligence : a modern approach*. Pearson.
- Salminen, A. (2011). *Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin*. Vaasan yliopisto.
https://www.uwasa.fi/materiaali/pdf/isbn_978-952-476-349-3.pdf
- Shekhar, S., Leder-Luis, J., & Akoglu, L. (2023). Unsupervised Machine Learning for Explainable Health Care Fraud Detection. NBER Working Paper Series.
<https://doi.org/10.3386/w30946>
- Strubell, E., Ganesh, A., & McCallum, A. (2020). Energy and policy considerations for deep learning in NLP. *ACL 2019 - 57th Annual Meeting of the Association for Computational Linguistics, Proceedings of the Conference*, 3645–3650.
- Sutton, R. S., Barto, A. G., & Bach, F. (2018). *Reinforcement learning : an introduction* (Second edition.). The MIT Press.
- Viaene, S., & Dedene, G. (2004). Insurance Fraud: Issues and Challenges. *Geneva Papers on Risk and Insurance. Issues and Practice*, 29(2), 313–333.
<https://doi.org/10.1111/j.1468-0440.2004.00290.x>
- Viaene, S., Dedene, G., & Derrig, R. A. (2005). Auto claim fraud detection using Bayesian learning neural networks. *Expert Systems with Applications*, 29(3), 653–666.
<https://doi.org/10.1016/j.eswa.2005.04.030>

4.5 Verkkolähteet

- Association of British Insurers. (2022). *Insurance fraud statistics 2022*.
<https://www.abi.org.uk/data-and-resources/industry-data/>
- Chy, J. (2024). *Proactive fraud defense: Machine learning's evolving role in protecting against online fraud*. ArXiv. <https://arxiv.org/abs/2410.20281>
- Coalition Against Insurance Fraud. (2021). *The impact of insurance fraud*.
<https://www.insuranceeurope.eu/mediaitem/0bf0af82-e7ef-4439-a763-d7862859d421/The%20impact%20of%20insurance%20fraud.pdf>
- EIOPA. (2021). *Artificial Intelligence governance principles: Towards ethical and trustworthy AI in the European insurance sector*.
https://www.eiopa.europa.eu/publications/artificial-intelligence-governance-principles-towards-ethical-and-trustworthy-artificial_en
- EITCA Academy. (n.d.). *What is the support vector machine (SVM)?*
<https://fi.eitca.org/artificial-intelligence/eitc-ai-mlp-machine-learning-with-python/support-vector-machine/svm-parameters/what-is-the-support-vector-machine-svm/>
- Euroopan parlamentti. (2020, elokuu 27). *Mitä tekoäly on ja mihin sitä käytetään?*
https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804_fi.pdf
- European Parliament. (2020). *Tackling fraud in the EU: Healthcare sector*.
https://www.europarl.europa.eu/pdfs/news/expert/2020/9/story/20200827STO85804/20200827STO85804_fi.pdf
- Finanssiala ry. (2023). *Vakuutuspetos on rikos – ja rikoksella on seuraamuksia: yhtiöiden tutkinnassa viime vuonna 2 500 epäselvää vahinkoilmoitusta*.
<https://www.finanssiala.fi/uutiset/vakuutuspetos-on-rikos-ja-rikoksella-on-seuraamuksia-yhtioiden-tutkinnassa-viime-vuonna-2-500-epaselvaa-vahinkoilmoitusta/>
- Finanssivalvonta. (2024). *Toimintakertomus 2024: Vakuutussektorin hallinto ja valvonta*.
<https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/toimintakertomukset/toimintakertomus-2024/teemat/vakuutussektorilla-tarkasteltiin-hallintoa/>
- Gee, J., & Button, M. (2019). *The financial cost of healthcare fraud 2019*. Centre for Counter Fraud Studies, University of Portsmouth.
<https://www.crowe.com/uk/croweuk/-/media/Crowe/Firms/Europe/uk/CroweUK/PDF-publications/The-Financial-Cost-of-Fraud-2019.pdf>
- IAIS (International Association of Insurance Supervisors). (2021). *Application paper on fraud in insurance*.

https://www.iaisweb.org/uploads/2022/01/Application_paper_on_fraud_in_insurance.pdf

- Infosys. (2023). *Harnessing the power of artificial intelligence in fraud detection*.
<https://www.infosys.com/industries/insurance/documents/artificial-intelligence-fraud-detection.pdf>
- Insurance Europe. (2013). *The impact of insurance fraud*.
<https://www.insuranceeurope.eu/mediaitem/0bf0af82-e7ef-4439-a763-d7862859d421/The%20impact%20of%20insurance%20fraud.pdf>
- Insurance Europe. (2019). *Insurance fraud: not a victimless crime*.
<https://www.insuranceeurope.eu/mediaitem/2bf88e16-0fe2-4476-8512-7492f5007f3c/Insurance+fraud+-+not+a+victimless+crime.pdf?inline=1>
- Insurance Europe. (2024). *Annual Report 2023–2024*.
<https://reports.insuranceeurope.eu/annual-report-2023-2024>
- Insurance Fraud Bureau. (2024). *Annual fraud report 2024*.
<https://www.insurancefraudbureau.org/media/1ovgb2eq/ifb-annual-report-2024.pdf>
- Jyrinsalo, H. (2024). *Ajoneuvovakuutuspetosten havaitseminen teknologian avulla*. Kandidaatin tutkielma, Tampereen yliopisto. Trepo.
<https://trepo.tuni.fi/bitstream/handle/10024/156709/JyrinsaloHenna.pdf>
- Jyväskylän yliopisto. (n.d.). *Laadullinen tutkimus – Menetelmäpolku*.
<https://sites.app.jyu.fi/mehu/fi/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus>
- OECD. (2021). *Financial consumer protection and the digitalisation of financial services*. OECD Publishing. <https://www.oecd.org/finance/financial-consumer-protection-and-the-digitalisation-of-financial-services.htm>
- SAP SE. (n.d.). *Mitä koneoppiminen on?* <https://www.sap.com/finland/products/artificial-intelligence/what-is-machine-learning.html>
- SAS Institute. (2022). *Fraud detection and prevention – SAS Insights*.
https://www.sas.com/fi_fi/insights/fraud/fraud-prevention.html
- Tukonen, J. (2024). *Lohkoketjuteknologian rooli terveysturvakuutuspetosten tunnistamisessa ja ehkäisyssä*. Kandidaatin tutkielma, Tampereen yliopisto. Trepo.
<https://trepo.tuni.fi/bitstream/handle/10024/162377/TukonenJanette.pdf>

4.6 Oikeudelliset lähteet

Euroopan parlamentti ja neuvosto. (2016). *Euroopan unionin yleinen tietosuoja-asetus (GDPR), artikla 22.*

Rikoslaki (39/1889)