Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

SEVERI LEHTIMÄKI

Tekoälyn mahdollisuudet ja uhat henkilötietojen käsittelyssä

LIIKETALOUDEN TUTKINTO-OHJELMA
2024

TIIVISTELMÄ

Lehtimäki, Severi: Tekoälyn mahdollisuudet ja uhat henkilötietojen käsittelyssä
Opinnäytetyö, AMK
Liiketalous
Kesäkuu 2024
Sivumäärä: 39

Opinnäytetyön tavoitteena oli luoda perusymmärrys tekoälyn ja henkilötietojen käsittelyn ympärille luoden käsitystä siitä, että mitä eri tekoälyratkaisuja on jo luotu henkilötietojen käsittelyyn ja miten niitä voitaisiin tulevaisuudessa kehittää ottaen huomioon henkilötietojen suoja.

Perusymmärrystä alettiin luomaan tekoälyn ympärille historialla, josta siirryttiin nykyaikaiseen tekoälyn käsittelyyn. Tämän jälkeen käsiteltiin tekoälyn peruskäsitteitä ja tarkasteltiin sen vahvuuksia, heikkouksia ja eettistä näkökulmaa.

Henkilötietojen ja GDPR osalta käsiteltiin henkilötietojen suojaamisen historiaa, josta siirryttiin GDPR keskeisiin periaatteisiin ja tavoitteisiin. Viimeisenä teoriaosuudessa käytiin läpi eri vaatimukset henkilötietojen käsittelyssä tekoälyn avulla.

Tarkoituksena oli luoda tutkimus, joka auttaa tekoälyn ja henkilötietojen käsittelyn käsitteiden ymmärtämistä samalla luoden käsitteiden välille yhteys. Yhteyden muodostuttua käsiteltiin niiden välillä olevia mahdollisuuksia ja uhkia.

Tutkimusta varten analysoitiin artikkeleita ja tutkimuksia sekä aiheisiin kuuluvaa kirjallisuutta. Tämän lisäksi käytiin läpi tutkimuskohteita nykyajan mahdollisuuksista ja haasteista. Taulukkoja käytettiin hyödyksi havainnoimaan monien eri osa-alueiden tekoälyratkaisuja.

Opinnäytetyön tuloksena luotiin perusta tekoälylle ja henkilötietojen käsittelylle. Analyysissa tuotiin esille nykyaikaisia tekoälyratkaisuja ja niihin kohdistuvia mahdollisuuksia ja uhkia henkilötietojen käsittelyssä.

Avainsanat: tietotekniikka, tekoäly, henkilötietojen suoja, GDPR

ABSTRACT

Lehtimäki Severi: The possibilities and threats of artificial intelligence in the processing of personal data
Bachelor’s thesis
Business economics
June 2024
Number of pages: 39

The aim of the thesis was to create a basic understanding around artificial intelligence and the processing of personal data, creating an understanding of what different artificial intelligence solutions have already been created for processing personal data and how they could be developed in the future, considering the protection of personal data.

A basic understanding of artificial intelligence with history, from which we moved on to the modern handling of artificial intelligence. After that, the basic concepts of artificial intelligence were discussed and its strengths, weaknesses and ethical perspectives.

Regarding for personal data and the GDPR, the history of personal data protection was discussed, from which we moved on to the GDPR’s central principles and goals. Finally, in the theory part, the different requirements for processing personal data with the help of artificial intelligence were reviewed.

The purpose was to create research that helps the understanding of the concepts of artificial intelligence and personal data processing while creating connection between these two concepts. After the connection was formed, the opportunities and threats between them were discussed.

For the research, articles and studies as well as literature related to the topics were analyzed. In addition to this, we went through research topics about the possibilities and challenges of today. The tables were useful to observe artificial intelligence solutions in many different areas.

As a result of the thesis, a foundation was created for artificial intelligence and personal data processing. The analysis highlighted modern artificial intelligence solutions and the opportunities and threats facing them in the processing of personal data.

Keywords: computer technology, artificial intelligence, personal data protection, GDPR

SISÄLLYS

1 JOHDANTO

Tämän työn aiheena on Tekoälyn mahdollisuudet ja uhat henkilötietojen käsittelyssä. Opinnäytetyö on toteutettu tutkimuksellisena aiheanalyysinä. Työn tarkoituksena on analysoida tutkimuksia tähän aihepiiriin liittyen ja luoda näistä tietopohja ja päätelmiä henkilötietojen käsittelyyn tekoälyn avulla liittyen.

Aiheen valintaan vaikutti tämän aihepiirin ajankohtaisuus ja omanlainen murrostila henkilötietojen käsittelyn tulevaisuudesta. Tekoälyä itsessään on jo käsitelty moneen otteeseen kirjallisuuskatsauksena, niin myös henkilötietojen suojaa, eli GDPR, mutta kun tarkastellaan näkökulmasta, jossa henkilötietoja käsitellään tekoälyn avulla, huomataan ettei näiden yhtäläisyyksistä ole tehty samalla tavalla tutkimuksia. Opinnäytetyö keskittyy tekoälyn, tietosuojan ja lainsäädännön yhtenäisyyksiin. Tekoäly kehittyy nopeaa tahtia, joten tietoturvan on pysyttävä perässä monien eri epäoikeudenmukaisten tilanteiden estämiseksi. Tavoitteena luoda perusymmärrys tekoälyn ja henkilötietojen käsittelyn ympärille samalla luoden käsitystä siitä, että mitä eri tekoälyratkaisuja on jo luoto henkilötietojen käsittelyyn ja miten niitä voitaisiin tulevaisuudessa kehittää ottaen huomioon henkilötietojen suoja.

Tutkimuskysymykset:

- Minkälaisia vahvuuksia tekoälyllä on henkilötietojen käsittelyyn liittyen ja mitkä asiat voivat horjuttaa näitä?
- Kuinka pitkälle tekoälyratkaisujen kanssa voidaan mennä vaarantamatta henkilötietojen suojaa?

2 TEKOÄLY

Tässä luvussa syvennytään tekoälyn historiaan, tiedealan kehityksen eri vaiheisiin ja sen nykytilaan jatkuvasti kehittyvässä maailmassa. Luvussa käsitellään tekoälyn eri osa-alueita ja toimintatapoja samalla pitäen katse tulevaisuudessa ja sen tuomista mahdollisuuksista.

2.1 Historia, kehityksen vaiheet ja nykytila

Tekoäly (”Artificial Intelligence”) on itsessään suhteellisen nuori tiedeala johtaen juurensa noin 70 vuotta ajassa taaksepäin. (Council of Europe, 2024)Vuosien varrella tekoäly on nähnyt paljon ylä- sekä alamäkiä ja historiassa on selvästi tunnistettavissa alan nopeita ja hitaita ajankohtia. (Kolari & Kallio, 2023, s. 18) Tekoäly yleensä mielletään vaikeasti määriteltäväksi tiedealaksi, mutta peruskäsitteenä tekoäly jäljittelee ihmisen kaltaista ajattelua ja toimintaa. (Kolari & Kallio, 2023, s. 14). Tekoälyn kehittyminen nykyaikaiselle tasolle on ollut vuoristorataa alusta alkaen ja siispä on tärkeää suunnata katse tämän tiedealan alkutaipaleelle ja kehityksen virstanpylväisiin.

2.1.1 Tekoälyn synty ja alkuinnostus

Tekoäly, eli tietoa käsittelevä kone on ollut ajatuksen tasolla jo antiikin ajoista lähtien, mutta varsinainen historia alkoi 1940- ja 1950-luvuilla. Historian alun selittää näihin aikoihin ensimmäisten digitaalisten tietokoneiden käyttöönotto (Kolari & Kallio, 2023, s. 18)

Ennen tekoäly termin varsinaista syntymistä John Von Neumann ja Alan Turing kehittivät tietokoneita mahdollistaen tekoälyn käyttöönoton. Desimaalilogiikka, joka käsittelee lukuja 0–9 ja binäärijärjestelmä, joka tukeutuu Boolean Algebraan, eli 2 kantalukuun, jotka ovat normaalisti luvut 0 ja 1. Näiden järjestelmien käyttöönotolla Neumann sekä Turing todistivat, että

tietokoneet ovat universaaleita, jotka pystyvät suorittamaan niille suunnattuja ohjelmia. (Council of Europe, 2024)

Varsinainen termi tekoäly syntyi kesällä vuonna 1956 Darthmound Collegessa John McCarthyn kutsuessa ”ajattelivista koneista” kiinnostuneita matemaatikkoja. John McCarthy esitteli matemaatikoille termin tekoäly ”artificial intelligence”, jota hän itse oli käyttänyt jo hetken aikaa. Termistä muodostui työpajan päättymisen myötä uuden tieteenalan nimi. (Kolari & Kallio, 2023, s. 18)

Darthmouth Collegessa muodostettiin monia optimistisia ajatuksia tekoälyn tulevaisuudesta. Kantavimpana ajatuksena pidettiin oppimisen ja älykkäiden toimintojen piirteiden kuvaamista niin, että kone voidaan ohjelmoida jäljittelemään niitä. (Kolari & Kallio, 2023, s. 18) Kuitenkaan 1950-luvun tietokoneet eivät olleet vielä tällä tasolla, koska kaapin kokoisten laskukoneiden muistiin mahtui suunnilleen yhden A4-arkin verran tekstiä. (Järvinen, 2023, s. 54) Tästä huolimatta tutkijat uskoivat, että koneet voidaan saada oppimaan ja ymmärtämään esimerkiksi kirjoitettua kieltä. (Kolari & Kallio, 2023, s. 18)

Ensimmäinen työpaja Darthmouth Collegessa oli erittäin hedelmällistä aikaa uuden tieteenalan alulle. Matemaatikot Allen Newell ja Herbert Simon esittelivät Logic Theorist-ohjelman, joka pystyi jo todistamaan monimutkaisia matemaattisia teoreemia. (Kolari & Kallio, 2023, s. 18) Tämän ohjelman jälkeen seurasi monia muita tiedealalle merkittäviä keksintöjä, esimerkiksi tekoäly Eliza.

Eliza on Joseph Weizenbaumin vuonna 1966 kehittämä ohjelma, joka tekee ihmisen ja tietokoneen välisen keskustelun mahdolliseksi. Ohjelma toimii niin, että syötettyä lausetta analysoidaan käyttämällä hajoamissääntöä, eli skriptiä, joka aktivoituu havaitsemalla avainsanoja syötetystä tekstistä. Vastaukset tuotetaan yhdistelemällä käytettyjä sääntöjä skriptissä. (Weizenbaum, 1966) Ohjelman tunnetuin skripti on psykiatria matkiva DOCTOR. Skriptissä ohjelma poimii syötetystä tekstistä avainsanoja, jonka jälkeen se tulostaa ne hieman muunneltuina kysymyksen muodossa. (Järvinen, 2023, s. 54) ELIZA on tiettävästi ensimmäinen ohjelma, joka yritti teeskennellä olevansa ihminen,

tästä johtuukin monien samankaltaisten ohjelmien suosio vuosien saatossa. Ohjelman suosion räjähtäessä Weizenbaum yritti selittää, ettei kone oikeasti osannut keskustella, vaan oli yksinkertainen ohjelma, joka muokkasi käyttäjän kirjoittamaa tekstiä ja tulosti sen näytölle. ELIZAn suuri suosio osoittaa sen, että kone onnistuu huijaamaan ihmistä, koska ihminen odottaa inhimillisien vastauksien tulevan toiselta ihmiseltä.

2.1.2 Tekoälyn kehityksen talvet

Tekoälyn tiedealalle on ominaista suurien innostusten aikakaudet ja niitä seuraavat romahdukset. Tiedealan sykliset nousut ja varsinkin laskut ovat leimanneet alaa jo pitkään, jonka ympärille on muodostunut käsitys tekoälyn talvet. Termillä viitataan tekoälyn ajanjaksoihin, jolloin kehitys epäonnistui tai hidastui merkittävästi. (Kolari & Kallio, 2023, s. 20)

Tekoäly oli alkuvuosinansa hyvin pitkälti tutkimustyörahoitteinen, koska markkinoita ei vielä ollut. Ensimmäisiä isompia tutkimuskohdehankkeita oli koneellinen kielenkääntö, jonka tutkiminen alkoi 1950-luvulla. Yhdysvaltojen hallitus oli kiinnostunut tietokoneen mahdollisuuksista kääntää venäjänkielisiä dokumentteja englanniksi, mutta tutkimus osoittautui pettymykseksi. Tietokone oppi kääntämään sanoja mekaanisesti, mutta tämä ei riittänyt sanojen erilaisista merkityksistä eri asiayhteyksissä. Tämän takia tutkimuksen rahoitus lakkautettiin vuonna 1966, joka oli suuri takaisku tiedealalle.

Ensimmäisestä isommasta takaiskusta huolimatta tekoälyn rahoitukset jatkuivat muissa hankkeissa suurimmaksi osaksi DARPAn (the U.S. Defense Advanced Research Projects Agency) ja rahoittamana. DARPA rahoitti vuodesta 1956 vuoteen 1974 monia hankkeita esimerkiksi ohjelmaa, joka osasi pelata tammea. (Lutkevich, 2022). Vuodet 1973 ja 1974 olivat kohtalokkaita tekoälyn kehityksen jatkolle. Vuonna 1973 julkaistiin akateeminen tutkimus tekoälyn tiedealasta nimeltään ”Lighthill Report”. Raportti käsitteli kriittisesti tekoälyä tiedealana ja varsinkin sen suurenmoisia tavoitteita ja niiden epäonnistumisia. Raportti oli niin vaikutusvaltainen, että

Iso-Britannian tutkimusjärjestö katkaisi tekoälytutkimusten rahoittamisen. (Lutkevich, 2022) Heti seuraavana vuonna 1974 DARPA vetäytyi kaikesta tekoälyn rahoituksesta. Syynä vetäytymiseen oli tutkimusten epäonnistuminen tietokoneiden liian vähäisen laskentatehokkuuden takia. Vuodesta 1974 alkoi tekoäly tiedealan virallinen ensimmäinen talvi, joka kesti aina vuoteen 1980.

Tekoälyn ensimmäinen talvi kesti noin 6 vuotta, jonka jälkeen 1980-luvulla alkoi trendikäs asiantuntijajärjestelmien kehittäminen ja käyttöönotto. Asiantuntijajärjestelmiä kehitettiin moniin rajattuihin käyttötarkoituksiin, kuten lääketieteelliseen diagnostiikkaan. (Kolari & Kallio, 2023, s. 20) Kuuluisimmat lääketieteeseen kohdistetut asiantuntijajärjestelmät olivat MYCIN, käytettiin bakteeritartuntojen tunnistamiseen, DENDRAL, kemiallisten yhdisteiden molekyylirakennetta ennustava ja PXDES, keuhkosyövän tyyppiä ja leviämisastetta arvioiva. (Järvinen, 2023, s. 58)

Asiantuntijärjestelmät eivät olleet ainoita tekoälyyn miellettyjä tutkimuskohteita 1980-luvulla. Japani oli menestynyt 1970-luvulla kulutuselektroniikan markkinoilla ympäri maailmaa, mutta Japanin hallitusta huoletti tulevaisuus mikroprosessien ja tietokoneiden parissa, nimittäin japanin kieli graafisin merkkeineen ei taipunut 1980-luvun syöttö- ja tulostuslaitteisiin. (Järvinen, 2023, s. 59)

Näiden asioiden innoittamana Japanin kansainvälisen kaupan ja hallinnon ministeriö yhteistyössä 8 johtavan tietotekniikka yrityksen kanssa lanseerasi tutkimusohjelman tietokoneohjelmista 1990-luvulle. Tätä projektia kutsuttiin ”Fifth Generation”, jonka kestoksi asetettiin 10 vuotta. (Ehud Y., 1983) Projekti perustuisi satojen tai jopa tuhansien prosessorien rinnakkaisuuteen. Tämä tarkoittaisi sitä, että koneet voisivat suorittaa samanaikaisesti suuria määriä käskyjä, joka tehostaisi niiden suoritustehoa moninkertaiseksi. Projekti epäonnistui asettamissaan tavoitteissaan sen hetkisen tietotekniikan tehottomuuden takia, joten Japani pysäytti rahoituksen tutkimukselle.

Ennen Japanin tekoälytutkimuksen lopettamista tiedeala oli nähnyt monia romahduksia ja leikkauksia, jotka yhdessä aiheuttivat tiedealan toisen merkittävän talven.

2.1.3 Tekoäly nykypäivänä

Takatalvista ja muista takaiskuista huolimatta tekoäly palasi entistä vahvempana datan määrän valtaisan kasvun (big data) ja tietokoneiden laskentakapasiteetin kehittymisen ansiosta. Yksi suurimmista syistä tekoälyyn perustuvien ratkaisujen, koneoppimisen ja neuroverkkojen yleistymiselle oli laskentatehon kasvu. Laskentatehon räjähdysmäinen kasvu mahdollisti yhden suurimmista keksinnöistä, neuroverkot, jotka kykenevät hyödyntämään grafiikkakiihdyttimien laskentakapasiteetin ja massadatan niiden laajuudessaan. Neuroverkkojen parissa työskennelleet yritykset ovat pystyneet toiminnon avulla luomaan tekoälyohjelmia, jotka pystyvät tuottamaan luonnollista kieltä, vastaamaan haastavampiinkin kysymyksiin ja käskystä luoda kuvia. (Kolari & Kallio, 2023, s. 21)

Kilpailu on kovaa ja uusia tekoälyohjelmia luodaan nopealla tahdilla. Tällä hetkellä tekoäly, varsinkin luova tekoäly voidaan jakaa karkeasti viiteen kategoriaan, sisällöntuottajat, tiedonpoimijat, älykkäät chatbotit, kieltenkääntäjät ja koodigeneraattorit. (Järvinen, 2023)

Sisällöntuotannon ala on jo päässyt kokemaan tekoälyn mullistavan voiman. Tämä kategoria pitää sisällään tekoälysovelluksia, jotka voivat tuottaa monipuolista sisältöä, kuten blogikirjoituksia, sähköposteja, sosiaalisen median julkaisuja, kuvia, videoita ja jopa 3D-malleja. Nämä sovellukset ovat kehitetty niin pitkälle, että ne eivät ainoastaan tuota sisältöä, vaan mukautuvat ja oppivat
käyttäjänsä tyylin ja mieltymyksen mukaan. (Järvinen, 2023)

Tiedonpoimija-sovellukset ovat elintärkeä apu tiedontäyteisessä maailmassa. Nämä sovellukset ovat tärkeässä asemassa suurien tietomäärien

suodattamisessa, analysoimisessa ja tiivistämisessä, jotta käyttäjät voivat saada olennaisen tiedon nopeasti ja vaivattomasti. Yleisesti ottaen tiedonpoimijat ovat oikeudellisten asiakirjojen, kirjojen ja muiden laajojen dokumentaatioiden käsittelyssä todella taitavia ja nopeita. (Järvinen, 2023)

Älykkäät chatbotit ovat mullistaneet vuorovaikutuksen ihmisten ja koneiden välillä. Ne osaavat tuottaa luonnollista kieltä ja käydä keskusteluja ihmisten kanssa. Chatbotteja käytetään runsaasti asiakaspalvelussa, koska heiltä asiakas saa nopeasti, tarkasti ja kellonajasta riippumatta apua arkisiin kysymyksiin liittyen.

Kielenkääntäjät ovat tärkeä sovellusalue luovalle tekoälylle. Tekoälysovellukset kykenevät kääntämään tekstiä monille eri kielille, joka on monikielisille kansainvälisille yrityksille hyödyllinen työkalu. Nämä työkalut käyttävät monimutkaisia algoritmeja ja koneoppimista tuottaakseen tarkkoja ja luonnollisia käännöksiä halutusta tekstistä. (Järvinen, 2023)

Koodigeneraattorit ovat luovan tekoälyn sovelluksia, joiden avulla ohjelmistokehityksen ala on tehostunut ja monipuolistunut huomattavasti. Sovellukset voivat tuottaa koodia eri ohjelmointikielillä ja auttaa tunnistamaan ja korjaamaan koodauksessa tulleita virheitä. Niillä on myös tekoälylle ominainen tapa oppia ja mukautua ohjelmistokehittäjien tyyleihin ja mieltymyksiin, joka yleensä auttaa koodin luettavuudessa ja ylläpidettävyydessä. (Järvinen, 2023)

2.2 Tekoälyn peruskäsitteet

Tekoäly yleiskäsitteenä on monille tuttu, mutta tekoälyyn sisältyy suuri määrä eri osa-alueita ja termejä. Tässä luvussa avataan tekoälyn peruskäsitteitä niin kuin koneoppiminen, neuroverkot ja syväoppiminen. Tämän luvun pohjalta lukijalle muodostuu peruskäsitys tekoälyn eri toimintatavoista.

2.2.1 Koneoppiminen

Jos olet joskus käyttänyt selaimesi hakukonetta, katsonut sosiaalisesta mediasta sisältöä tai katsonut joltain striimauspalvelulta elokuvia tai sarjoja, olet huomaamattasi käyttänyt koneoppimisen tuotoksia hyödyksesi. Hakukoneessa ennakoiva tekstinsyöttö, sosiaalisessa mediassa juuri sinulle kohdistettu sisältö ja striimauspalveluissa ehdotetut elokuvat tai sarjat, nämä kaikki edellä mainitut ovat koneoppimisen tuotoksia. Koneoppiminen on osa nykyaikaa ja sitä käytetään tosi laajalla alalla.

Koneoppiminen on yksi tekoälyn osa-alueista. Koneoppimisessa mitataan ohjelman kykyä parantaa omaa toimintaansa oppimalla itsenäisesti datasta niin, että toimintaa ei ole ohjelmoitu kokonaan valmiiksi. (Kolari & Kallio, 2023, s. 128) Koneoppiminen jakautuu yleisesti 3 eri pääosa-alueeseen: ohjattu oppiminen, ohjaamaton oppiminen ja vahvistettu oppiminen.

Ohjattu oppiminen on muita koneoppimisen osa-alueita suoraviivaisempi. Tässä osa-alueessa koneelle annetaan koulutusdataa halutusta lopputuloksesta ja sen perusteella kone etsii datasta piirteitä ja niihin perustuvia sääntöjä, joiden avulla päästään parhaiten haluttuun lopputulokseen. Esimerkkinä kasvojen kuvat ja niille annetut henkilöiden nimet. Koneelle annetaan tiedot jokaisen kuvan oikeasta nimestä, jonka yhteydessä kone onnistuneessa oppimisessa opettelee kasvoihin liittyviä erityispiirteitä. Kun koneelle on opetettu tarpeeksi aineisto, voidaan suorittaa viimeinen vaihe. Koneelle syötetään dataa, jossa on jo opeteltua ja opettelematonta dataa, jonka jälkeen tarkastellaan, miten kone käsittelee tilanteen. Jos kone on oppinut oikein se osaa isolla todennäköisyydellä nimetä oikein opetettuja kasvokuvia. (Kolari & Kallio, 2023, s. 129)

Ohjaamaton oppiminen on täysin päinvastainen koneoppimistyyli kuin ohjattu oppiminen. Ohjaamattomassa oppimisessa ei käytetä koulutusdataa piirteiden ja sääntöjen muodostamiseen. Koneelle annetaan yleensä laajempia kokonaisuuksia lopputuloksen muodostamiseen. Koneelle voidaan antaa esimerkiksi ryhmittely tehtävä, jossa monimutkaista dataa ryhmitellään helpommin visualisoitavaksi. (Kolari & Kallio, 2023, s. 130)

Vahvistettu oppiminen on ohjatun ja ohjaamattoman oppimisen välimaastossa. Koneelle ei suoraan anneta haluttuja lopputuloksia, vaan työkaluja sitä varten, esimerkiksi toimia, sääntöjä tai miten mahdollisesti päästä lopputulemaan. Kone selvittää, miten päästä lopputulokseen ja palkintojen avulla autetaan konetta ymmärtämään, mitä haluttua lopputulosta haetaan ja millä tavalla. (SAP SE, 2024)

2.2.2 Neuroverkot ja syväoppiminen

Neuroverkkojen idea on keksitty jo 1980-luvulla, mutta koneiden vähäisen muistin ja prosessoreiden tehottomuuden takia neuroverkkojen käyttöönotto ja rakentaminen viivästyi 2000-luvulle. Näihin aikoihin saatiin tekoäly ”oppimaan” itsekseen asioita, joiden opettaminen asia kerrallaan olisi vaatinut tähtitieteellisen määrän ihmistyötä. (Järvinen, 2023, s. 73)

Neuroverkko on tekoälyn yksi tärkeimmistä komponenteista. Neuroverkot jäljittelevät ihmisen aivojen toimintaa ja kykyä oppia. (Winter, 2024) Neuroverkot rakentuvat yksittäisten neuroneiden yhdistämisestä. Muodostuneen verkon läpi kulkeva data liikkuu neuronien välisiä yhteyksiä pitkin. (Kolari & Kallio, 2023, s. 131) Nämä yhteydet voivat toimia sekä vahvistavina, että heikentävinä tekijöinä, jotka määrittävät neuroverkon suhtautumisen tuleviin samankaltaisiin kytköksiin. (Winter, 2024)

Neuroverkon tapa oppia on koneoppimisen tyyppistä, eli opetusdatan ja opetusvaiheen tavoin. Opetusvaiheessa neuroverkolle annetaan jonkinlainen syöte, johon sen tulee antaa tietty vastaus. Neuroverkon antaessa väärän vastauksen säädetään sen painotuksia, eli neuronien välisiä yhteyksiä niin, että vastaus olisi mahdollisesti seuraavalla kerralla oikein. Opetusvaiheen jälkeen neuroverkkoa voidaan käyttää ennestään tuntemattomien syötteiden analysointiin. Neuroverkon tyypillisimpiä käyttökohteita ovat kuvan-, puheen- ja tekstin tunnistuksessa sekä taloudellisessa ennustamisessa, että pelitekoälyssä. (Winter, 2024)

Syväoppiminen on tekoälyn ja koneoppimisen osa-alue, joka hyödyntää aikaisemmin käsiteltyjä neuroverkkoja. Syväoppiminen hyödyntää neuroverkkoja monessa eri kerroksessa, joidenka kokonaisuutta kutsutaan usein syviksi neuroverkoiksi (engl. Deep Neural Networks = DNNs). (Metropolia Ammattikorkeakoulu, 2024)

Syväoppimisen myötä siirryttiin perinteisten yhden tai muutamien neuroverkkojen kerroksista kymmenien tai jopa yli sadan neuroverkoston kerroksiin. (Kolari & Kallio, 2023, s. 131). Jokaisella kerroksella on tärkeä tehtävä jalostaa ja tiivistää edellisen kerroksen antamaa informaatiota yhä kuvailevampaan suuntaan lopputulosta kohti. (Järvinen, 2023, s. 75) Esimerkiksi eläinten kuvien opettelussa ensimmäinen kerros voi tunnistaa reunoja, seuraava kerros reunoista muodostuvia alueita, siitä seuraava kerros alueista muodostuvia muotoja, seuraava kerros muodoista syntyviä hahmoja ja näiden kerroksien jälkeen seuraava kerros voi tunnistaa jo silmiä, korvia, häntiä ja tassuja. Eri kerrosten neuroneille annetaan arvot, joista suurimman arvon saanut neuroverkostosarja valikoituu ulostulokerroksessa käytettävään kuvan tulkintaan. (Järvinen, 2023, s. 75)

2.3 Vahvuudet, heikkoudet ja eettinen näkökulma

Koneiden, eli yleensä tekoälyn avulla monissa yrityksissä on tehostettua tiettyjä osa-alueita ja toimintoja. Kone on väsymätön työntekijä ja tilastollisesti vähemmän virheitä tekevä. Koneen kyvykkyydestä on monia esimerkkejä, mutta yksi kuuluisimmista on vuonna 1997 tapahtunut Deep Bluen, eli tekoälyn voitto sen ajan shakin maailmanmestari Garry Kasparovia vastaan. Kasparov hävisi toisen ottelunsa, koska häneltä jäi kriittinen siirto huomioimatta, joka olisi tuonut vähintään tasapelin hänelle. Vastaava kriittisen siirron huomioimattomuus ei tapahdu tekoäly. Se huomaa jokaisen hänelle opetetun mahdollisuuden. (Järvinen, 2023, s. 70) Vaikka tekoäly voi vaikuttaa ylivoimaiselta ihmiseen nähden on sillä monia puutteellisuuksia, johon ainoastaan ihmisen aivot pystyvät.

2.3.1 Vahvuudet ja heikkoudet

Jokaisessa vallankumouksellisessa keksinnössä on hyviä sekä huonoja puolia, joten niin on myös tekoälyssä. Tekoäly on tuonut paljon valtioille, yrityksille ja ihmisille, mutta sen riskeistä tulee harvoin puhuttua. Käsitellään muutamia tekoälyn vahvuuksia ja heikkouksia, jotta molemmista puolista saadaan riittävä käsitys nykyajan ja tulevaisuuden tekoäly toteutuksia varten.

Tableau:n sivuilla käsitellään tekoälyn vahvuuksia ja heikkouksia artikkelissa ”What are the advantages and disadvantages of artificial intelligence (AI)?”. Käsittelen tästä artikkelista 3 vahvuutena ja 3 heikkoutena pidettävää ominaisuutta tekoälyssä.
Ensimmäisenä ja jopa yksi isoimmista ominaisuuksista on tekoälyn vähäinen tai melkein olematon virheiden teko riippuen aineistosta. Inhimillisten virheiden sattuminen on melkein mahdotonta ihmisten tekemässä työssä, vaikka siihen kuinka panostettaisiin. Tekoälyn avulla monien palveluiden virheetön laatu ja kokemus auttavat asiakaskokemuksen parantamisessa ja tuotteiden valmistamisessa. Todella tärkeä vahvuus on myös ympäri vuorokautinen saatavuus. Tekoäly ei väsy, joten esimerkiksi asiakaspalvelurobotit voivat auttaa yrityksen aukioloaikojen ulkopuolella. Viimeisenä tärkeänä vahvuutena pidän tekoälyn kykyä kerätä, hallita ja analysoida suuria määriä dataa, josta se pystyy luomaan esitettävää tietoa helposti ymmärrettävässä muodossa.

Ensimmäisenä oleva heikkous on varsinkin tällä hetkellä ollut puheenaiheena nimittäin hintavat tekoälyn toimeenpano- ja käyttöönottomaksut. Tableau:n artikkelissa puhutaan yrityksien maksavan 20 000 eurosta moniin miljooniin euroihin riippuen tekoälytoiminnon laajuudesta. Tekoälyn kulut tulevat kuitenkin maksamaan itsensä takaisin tehostaessaan työtahtia. Seuraavana haluan nostaa artikkelista ylös tekoälyn tunteiden ja luovuuden puutteellisuus. Artikkelissa luovuuden puutteellisuus tarkoittaa, että opetetusta datasta poikkeavaa uutta ratkaisua ongelmaan ei ole tekoälyllä vielä mahdollista toteuttaa. Samaa pätee myös tekoälyn tunteiden puutteellisuuteen. Tekoäly tekee päätöksensä ainoastaan aineistoon viitaten, joten kaikki normaalin inhimillisen tunteen puutteellisuus tulee tässä esille. Viimeinen ja myös tämän

raportin aiheelle merkityksellinen heikkous, eettiset ongelmat. Tekoälyn käytön räjähdysmäinen kasvu on nostanut monia eettisen näkökulman kysymyksiä. Yksi tärkeimmistä on kuluttajien tietojen yksityisyys. Tekoälyn kehittyessä uudenlaiset ohjelmat voivat esimerkiksi tunnistaa kaavoja ihmisten yleisestä käyttäytymisestä ja tunnistaa henkilöitä ilman henkilökohtaisia tietoja.

2.3.2 Eettinen näkökulma

Tekoälyn viime vuosien kiihtyvä ja merkittävä kehitys on nostattanut puheenaiheeksi sen käytön eettiset seuraukset. Varsinkin, kun koneiden vastuut eri yhteiskunnan osa-alueilla ovat kasvaneet merkittäviksi. Eettisiä seurauksia pohtiessa on herännyt kysymyksiä tekoälyn hallinnasta, valvonnasta ja vastuusta. Näiden kysymysten perusteella on nähty tarpeelliseksi luoda eettisiä ohjeistuksia ja säännöstöjä, jotka takaavat tekoälyn turvallisen, vastuullisen ja oikeudenmukaisen käytön. (Salo, 2023, s. 17)

Eettistä näkökulmaa on tarkasteltu monesta eri kulmasta esimerkiksi itsemääräämisoikeus, datan käyttö, työelämän vaikutukset ja taloudellinen eriarvoisuus. Itsemääräämisoikeudessa on mietitty kuinka laajasti tekoälyllä olisi vapaus tehdä omia päätöksiä ja kuinka paljon ihmisten tulisi olla mukana tekemässä päätöksiä? Datan käytössä yksilön tietosuoja ja yleisesti datan hyödyntäminen kiinnostaa ja huolestuttaa ihmisiä, kuten kuka omistaa datan ja kuinka varmistutaan, ettei tekoäly vahingossa paljasta tai hyödynnä tietoja epäeettisellä tavalla? Työelämän vaikutuksissa on pohdittu, että minkälaiset työllisyys näkymät ja työnkuvat tulevaisuudessa tulee olemaan? Taloudellisessa eriarvoisuudessa palveluiden maksullisuus tulevaisuudessa saattaa laittaa ihmisiä eriarvoiseen asemaan.

3 HENKILÖTIETOJEN SUOJAAMINEN JA GDPR

Henkilötietojen suojaaminen korostuu vuosi vuodelta enemmän tietokoneiden ja tekoälyratkaisujen kehittyessä. Tietokoneet pystyvät käsittelemään entistä enemmän dataa ja taas tekoälyohjelmat pystyvät entistä paremmin ymmärtämään laajaa kirjoa erilaista dataa. Nykyaikaiset datan käsittelyohjelmat vaativat myös nykyaikaiset tietosuojalait varmistaakseen, että suuria määriä dataa kerätään, käsitellään ja säilötään oikealla tavalla ketään vaarantamatta. Tätä varten Euroopan komissio päivitti 24. toukokuuta 2016 tietosuojalainsäädäntöänsä turvatakseen ihmisten henkilötietojen käsittelyn jatkuvasti kehittyvässä maailmassa.

3.1 Henkilötietojen suojaamisen historia ja määrittely

Yleinen tietosuoja-asetus (GDPR) on laajasti yksityishenkilöiden henkilötietoja suojaava asetus, joka ei ole ilmaantunut tyhjästä. Tämä asetus on monien sopimusten ja projektien aikaansaannos, joka on saanut alkunsa toisen maailmansodan julmuuksien seurauksena. Yhdistyneet kansakunnat julistivat yleiskokouksessa 10.12.1948 yleismaailmalliset ihmisoikeudet, jonka 12 artiklassa määritellään yksityiselämän suojasta ja siihen liittyvistä oikeuksista. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 4) Yleismaailmallisten ihmisoikeuksien määreet ovat tarjonneet perustan eurooppalaiselle tietosuojalle. (Rudgard, 2019)

Tästä jatkui ihmisoikeuksien kehittäminen nimittäin vuonna 1950 Euroopan neuvosto laati yleissopimuksen ihmisoikeuksien ja perusvapauksien suojaamisesta (EIS). (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 4)Yleissopimus sitoo allekirjoittaneita Euroopan neuvoston jäseniä, jonka

mukaan jäsenet vannovat vankkaa uskoaan oikeudenmukaisuuden ja maailmanrauhan perustana oleville ihmisoikeuksille, perusvapauksille ja näiden kehittämiselle. (Euroopan ihmisoikeussopimus 63/1999, ei pvm) EIS 8 artikla sisältää samanlaisen julistuksen kuin Yhdistyneiden kansakuntien ihmisoikeuksien artikla 12 ihmisten yksityisyyden suojasta. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 4) Tässä artiklassa mainitaan jokaisen oikeudesta nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta ilman, että viranomaiset puuttuvat tämän oikeuden käyttämiseen, pois lukien erikseen määritellyt tilanteet.

Useat Euroopan maat alkoivat jo 1960- ja 70-luvuilla säätämään henkilötietojen käsittelyä koskevia lakeja. Vaikka tietotekniikka olikin silloin vasta alkuvaiheissaan, kasvoi huoli uuden teknologian mahdollisuudesta vaarantaa ihmisen yksityisyys. Huolenaiheeseen vastaten Euroopan neuvoston parlamentaarisessa yleiskokouksessa annettiin vuonna 1968 suositus 509, jossa määriteltiin periaatteet ja normit henkilötietojen epäoikeudenmukaisen käsittelyn estämiseksi. Näiltä ajoilta on säilynyt nykyiseen tietosuojalainsäädäntöön muun muassa oikeus tietää omien henkilötietojensa käsittelystä, vaatimus tietojen oikeellisuudesta ja ajantasaisuudesta, säilytysaikojen rajoittaminen sekä käyttötarkoitussidonnaisuus (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 5)

OECD (Organisation for Economic Co-operation and Development) julkaisi vuonna 1980 ensimmäisen ohjeistuksensa yksityisyyden suojasta ja henkilötietojen rajatylittävästä siirtämisestä. (OECD, 1980) Ohjeistus ei ole sitova, mutta sillä on ollut pitkäaikaisia vaikutuksia tietosuojalainsäädännön kehitykseen. Vuonna 1981, eli vuosi OECD ohjeistuksen julkaisemisen jälkeen Euroopan neuvosto hyväksyi yleissopimuksen (yleissopimus 108) yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä, joka oli ensimmäinen oikeudellisesti sitova sopimus henkilötietojen suojaamisesta. Perusperiaatteiltaan yleissopimus 108 muistutti paljon OECD:n ohjeistusta. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 6)

Yleissopimus 10 ja OECD:n ohjeistus tähtäsivät yhdistämään kansallista lainsäädäntöä, mutta monien maiden kohdalla päädyttiin hyvin erilaisiin ratkaisuihin tietosuojaa koskevissa lainsäädäntöratkaisuissa. Niinpä Euroopan parlamentti pyysi komissiota valmistelemaan ehdotusta henkilötietodirektiivistä. Kahden vuosikymmenen uurastamisen ja valmistelun jälkeen lokakuussa vuonna 1995 hyväksyttiin direktiivi 95/46/EY. Direktiivi rakentui pitkälti yleissopimus 108 periaatteisiin ja sillä oli tavoitteena yksityisyyden suojan parantaminen, että vapaampi tietojen liikkuminen jäsenmaiden välillä. Direktiivin astuessa voimaan kansalliset lainsäätäjät saivat kuitenkin kohtuuttoman paljon liikkumavaraa direktiivin asettamien velvoitteiden toteuttamisessa, joten monien jäsenmaiden kohdalla tietosuojalainsäädännön yhdistäminen jäi vähäiseksi. Tämä nostatti tarpeen viedä direktiiviä pidemmälle, joka toimi pohjana nykyisen tietosuoja-asetuksen säätämiselle. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 7)

Tietosuoja-asetuksen keskeisin termi on henkilötiedot ja niiden käsittely, mutta siitä huolimatta monille jää kapea käsitys siitä, mitä henkilötiedot oikeasti pitävät sisällään. Tietoarkisto (Tietoarkisto, 2024) jaottelee henkilötietojen aineistot kolmeen eri ryhmään, suorat tunnisteet, vahvat epäsuorat tunnisteet ja epäsuorat tunnisteet. Suorat tunnisteet ovat kriittisimpiä henkilötietoja, koska niistä henkilö pystytään yksiselitteisesti tunnistamaan. Näitä tunnisteita ovat nimi, henkilötunnus, kasvot sisältävä valokuva, biometriset tunnisteet ja nimen mukainen sähköpostiosoite. Toisinaan vahvat epäsuorat tunnisteet nimensä mukaisesti eivät suoraan anna tarkkoja henkilöitä tunnistavia tietoja, mutta niiden avulla rajatulla määrällä ihmisiä on mahdollisuus tunnistaa henkilöitä yksiselitteisesti. Näitä tunnisteita ovat esimerkiksi pankkitilin numero, tietokoneen ip-osoite, opiskelijanumero, puhelinnumero, harvinainen ammattinimike, asema, joka voi olla vain yhdellä henkilöllä kerrallaan ja harvinainen sairaus. Epäsuorat tunnisteet ovat henkilötietoja, joita yhdistelemällä henkilö on mahdollista tunnistaa. Tässä ryhmässä yksi tieto ei riitä henkilön tunnistamiseen. Näitä tunnisteita on paljon, mutta tässä muutama esimerkki ikä, sukupuoli, etninen tausta, tulot, asuinkunta, postinumero, syntymäaika, ammatti, työnantaja. Kaikkien edellä mainittujen tietojen käsittely

turvallisesti, lainsäädäntöä ja direktiiviä noudattaen on elintärkeää tietosuojan turvallisuuden ja luotettavuuden varmistamiseksi.

3.2 GDPR keskeiset periaatteet ja tavoitteet

Yleinen tietosuoja-asetus (GDPR) on merkittävin yksittäinen asetus tietosuojaan liittyen. Sen merkitys kasvaa entisestään yhteiskuntarakenteiden ja tekoälyn kehittyessä. Tässä luvussa käydään läpi keskeiset yleisen tietosuoja-asetuksen periaatteet ja sen tavoitteet.

3.2.1 Tietosuoja-asetuksen periaatteet

Tietosuoja-asetuksen lähtökohtana ei ole ollut kaikkien henkilötietojen käsittelyyn liittyvien tapauksien ehdoton sääntely, vaan tietojen käsittelyn yhteydessä ohjaamassa ovat periaatteet, jonka puitteissa rekisterinpitäjät voivat suhteellisen vapaasti valita omat toimintatapansa. Periaatteet ovat loistavana apuna muuten monimutkaisen artiklan tulkitsemisessa. Yksittäisten säännösten ymmärtäminen voi olla välillä vaikeaa, mutta periaatteet tuntien ja muuten ymmärtäen tietosuoja-asetuksen kokonaisuuden, säännösten tulkitseminen helpottuu huomattavasti. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 28)

Periaatteita käsitellään TSA artikla 5. Artiklan mukaan käsittelyn tulee olla lainmukaista, eli sillä tulee olla lainmukaiset perusteet. Asetuksen mukaiset perusteet ovat rekisteröidyn suostumus, sopimus, rekisterinpitäjän lakisääteinen velvoite, elintärkeiden etujen suojaaminen, yleistä etua koskeva tehtävä tai julkinen valta sekä rekisterinpitäjän tai kolmannen osapuolen oikeutettu etu. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 28) Henkilötietojen käsittely tulee olla muutenkin laillista ja käsittelyn yhteydessä tulee aina olla varma tietosuojaperiaatteiden sekä muiden käsittelyä koskevien

vaatimusten ja periaatteiden asianmukainen toteutuminen. (Tietosuojavaltuutetun toimisto, 2024)

Asianmukaisuus periaate tarkoittaa, että henkilötietojen käsittelyn tulee olla asianmukaisesti ja kohtuullisesti toteutettu käsittelyn tarkoitukseen nähden. Henkilötietojen käsittelystä tulee kertoa riittävän selkeästi ja ymmärrettävästi eikä käsittelystä annettu tieto saa olla harhaanjohtavaa. Henkilötietojen käsittelyä ei saa peitellä eikä tietoja saa antaa rekisteröidylle manipuloivalla tavalla. (Tietosuojavaltuutetun toimisto, 2024)

Läpinäkyvyys periaate perustuu siihen, että rekisteröidyille kerrotaan selvästi mitä ja miten heidän tietojansa kerätään, käytetään tai muutoin käsitellään. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 29) Tietojen on oltava helposti saatavilla kuin myös helposti ymmärrettävissä. Nämä edesauttavat rekisterinpitäjän luotettavuuteen. (Tietosuojavaltuutetun toimisto, 2024)

Käyttötarkoitussidonnaisuuden periaate rajaa rekisterinpitäjän mahdollisia käyttökohteita kerättyjen henkilötietojen kohdalla. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 29) Henkilötietojen käyttötarkoitus on suunniteltava ja määriteltävä selkeästi ennen niiden käsittelyn aloittamista. Käyttötarkoitus on vielä yksilöitävä, dokumentoitava ja kerrottava rekisteröidyille. Tämä auttaa rekisteröityä ymmärtämään, mihin hänen tietojaan tarvitaan, arvioimaan käyttötarkoituksen asianmukaisuutta ja päättämään, haluaako hän vaikuttaa hänen henkilötietojensa käsittelyyn. (Tietosuojavaltuutetun toimisto, 2024)

Tietojen minimoinnin periaate tarkoittaa, että henkilötietoja saa käsitellä vain silloin, kun se on tarpeellista käsittelyn tarkoituksen kannalta. (Tietosuojavaltuutetun toimisto, 2024) Rekisterinpitäjän tulee määritellä käsittelyn tarkoitus. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 29) Käsittelyä varten henkilötietojen tulee olla asianmukaisia, eli henkilötietojen avulla on mahdollista täyttää määritellyt käyttötarkoitukset, olennaisia, eli henkilötiedoilla tulle olla selvä yhteys määriteltyyn käyttötarkoitukseen ja rajoitettuja, eli vain käyttötarkoituksen omaisia henkilötietoja saa kerätä. (Tietosuojavaltuutetun toimisto, 2024) Henkilötietojen säilytysaika tulee olla

käyttötarpeen mukainen ja mahdollisimman lyhyt. Joissain tapauksissa rekisterinpitäjillä on lakiin perustuva velvollisuus säilyttää tietoja tietyn ajan. Säilyttämisen perusteiden lakatessa tiedot tulee poistaa. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 29)

Luottamuksellisuus ja turvallisuus periaatteet sisältävät nimensä mukaisesti henkilötietojen luottamuksellista ja turvallista käsittelyä. Rekisterinpitäjän tulee arvioida mahdollisia riskejä, organisaation tietosuoja- ja tietoturvaohjeistuksen tasoa sekä henkilötietojen teknistä suojausta. Suojatoimien riittävyyttä punnitaan olosuhteisiin ja riskeihin suhteutettuna. Suojatoimet ovat henkilötietojen luvattoman tai lainvastaisen käsittelyn sekä vahingossa tapahtuvan hävittämisen, tuhoutumisen tai vahingoittumisen estämiseksi. Henkilötiedot tulee olla suojattuna kaikessa niihin kohdistuvissa käsittelyissä ja toimivuutta mitataan säännöllisesti olosuhteisiin ja riskeihin suhteutettuna. (Tietosuojavaltuutetun toimisto, 2024)

Näiden aikaisemmin käsiteltyjen periaatteiden lisäksi rekisterinpitäjällä on osoitusvelvollisuus periaatteiden noudattamiseksi. Tätä toteutetaan esimerkiksi dokumentoimalla toimenpiteitä sekä tekemällä vaikutustenarviointia ja mahdollisia muita arviointeja. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 30)

3.2.2 Tietosuoja-asetuksen tavoitteet

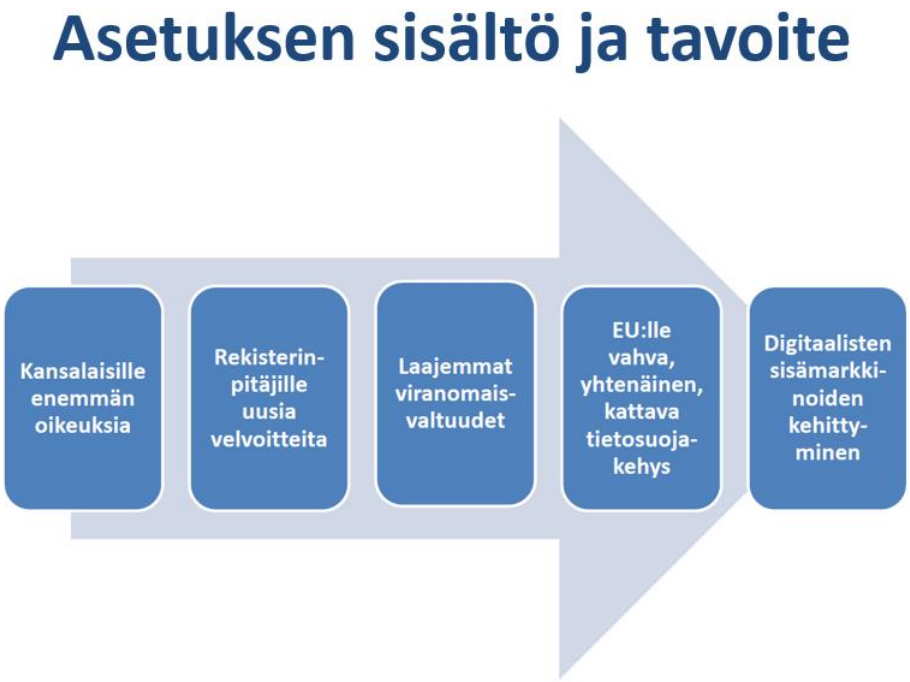
Jokaisella ihmisellä on oikeus omien henkilötietojen suojaan. Tätä puoltaa myös Euroopan unionin perusoikeuskirjan 8 artikla ja Euroopan unionin toiminnasta tehty sopimus (SEUT) 16 artikla. Periaatteissa ja säännöissä otettava huomioon ihmisten perusoikeudet ja -vapaudet katsomatta kansalaisuuteen tai asuinpaikkaan.

Tietosuoja-asetuksella on monia muitakin tehtäviä, kuten tukea vapauden, turvallisuuden, oikeusalueen ja talousunionin kehittämistä, taloudellista ja sosiaalista edistystä, talouksien lujittamista ja lähentämistä sisämarkkinoilla

sekä luonnollisten henkilöiden hyvinvointia. Erityistekijänä asetuksella yritetään tasapainottaa henkilön oikeuksia omiin tietoihinsa vaikeuttamatta yritysten ja muiden toimijoiden toimintaa henkilötietojen parissa. Toisin sanoen asetuksella ei yritetä estää henkilötietoihin perustuvaa liiketoimintaa, vaan tehdä lailliset puitteet ja määrittelyt, mikä henkilötietojen käyttö on sallittua ja mikä ei. Tästä hyvänä esimerkkinä on tietosuoja-asetuksen toteaminen, ettei henkilötietojen vapaata liikkumista unionin sisällä saa rajoittaa tai kieltää henkilötietojen käsittelystä johtuvista syistä. Tämä toteamus pyrkii auttamaan sisämarkkinoita myös henkilötietojen osalta. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 41)

Tietosuoja-asetuksen mukana tuli rekisterinpitäjälle paljon velvollisuuksia, mutta samalla näiden puitteissa henkilötietojen käsittely helpottui luonnollisin keinoin ja nopean teknologisen kehityksen avulla. Teknologisen kehityksen myötä alkoi esiintymään uusia haasteita. Nimittäin henkilötietoja jaetaan ja kerätään nykyään merkittävästi enemmän. Teknologian luotettavuutta henkilötietojen käsittelyssä auttaa vahva ja johdonmukainen tietosuojakehys tehokkaalla täytäntöönpanolla. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 43)

Edellä mainitut tavoitteet ovat olleet tietosuoja-asetuksen perusta ja näistä on myös maailmalla otettu mallia, koska tietosuoja-asetuksen voimaan astumisen jälkeen Kaliforniassa säädettiin ”California Consumer Privacy Act (CCPA)”, joka noudattaa pitkälti tietosuoja-asetuksen kohtia. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 44) Tavoitteet on vielä kuvitettu ja esitetty alla olevassa kuvassa, josta näkee asetuksen pääpiirteet nopealla vilkaisulla.



3.3 Vaatimukset henkilötietojen käsittelyssä tekoälyn avulla

Henkilötietojen käsittely ei ole perusoikeus. Henkilötietojen käsittelyyn liittyy vastuu henkilöille tärkeiden tietojen käsittelystä. Tätä varten yleisessä tietosuoja-asetuksessa on kattava määritelmä siitä, kenelle kuuluu tietojenkäsittelyketjussa erinäköiset vastuut.

3.3.1 Rekisterinpitäjän ja käsittelijän vastuut ja velvollisuudet

Henkilötietojen suoja on jokaisen ihmisen perusoikeus. Tämä johtaa siihen, että rekisterinpitäjillä ja henkilötietojen käsittelijöillä on suuri vastuu toteuttaa prosessi kohtuullisesti, läpinäkyvästi ja turvallisesti ilman, ettei mitään tunnistettavissa olevia henkilötietoja leviä henkilöille, joille ne eivät kuulu.

Tietosuojavaltuutetun toimiston sivustolla (2024) rekisterinpitäjäksi luokitellaan henkilö, yritys, viranomainen tai yhteisö, joka määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot. Rekisterinpitäjällä ja sen valtuuttamalla käsittelijällä on monia vastuita ja velvollisuuksia, joita käsitellään yleisellä

tasolla TSA 24 artiklassa. Vastuuseen liittyvää säännöstä tulee kuitenkin tulkita osana asetuksen kokonaisuutta ja sen tavoitteet huomioon ottaen.

Rekisterinpitäjän vastuita ja velvollisuuksia tulkitaan monen eri artiklan tietojen mukaan. TSA 82 artiklassa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän korvausvelvollisuudesta asetuksen vastaisen henkilötietojen käsittelyn johtaneesta vahingosta. Jokainen henkilötietojen asetuksen vastaiseen käsittelyyn osallistunut rekisterinpitäjä on yhteisvastuussa vahingosta syntyneen korvauksen hyvittämiseen. Siispä rekisterinpitäjällä on velvollisuus henkilötietojen käsittelyssä toteuttaa asianmukaiset ja tehokkaat toimenpiteet säännöksen ja lain noudattamisen varmistamiseksi.

Artikla 24 täydentää sopivasti TSA 5 artiklan 2 kohdassa ja aikaisemmin tässä raportissa mainittua osoitusvelvollisuutta. Tämä tarkoittaa sitä, että rekisterinpitäjän tulee voida osoittaa, että henkilötietojen käsittelytoimet ja niiden tehokkuus ovat asetuksen mukaisia. Toimenpiteiden edellytykset TSA 24 artiklan mukaan riippuvat käsittelyn luonteesta, laajuudesta, asiayhteydestä ja tarkoituksesta sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin liittyvistä riskeistä. Näihin toimiin vaikuttavat myös esimerkiksi TSA 5 artiklan 1 kohdan mukaiset periaatteet, joita käsitelty luvussa ”Tietosuoja-asetuksen periaatteet”.

Henkilötietojen käsittelijän määritelmä tulee TSA 4 artiklasta, jossa todetaan, että henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Tarkemmin henkilötietojen käsittelijästä käydään TSA 28 artiklassa. Rekisterinpitäjän halutessaan käyttää käsittelijää tulee henkilötietojen käsittelijän antaa riittävät takeet asianmukaisten teknisten ja organisatoristen toimien täytäntöönpanemiseksi, jotta käsittely täyttää asetuksen mukaiset vaatimukset ja rekisteröidyn tietojen suojelun.

Käsittelijä todistaa riittävät suojatoimet esittämällä dokumentaatioita prosessista. Näitä ovat esimerkiksi erilaiset sisäiset ohjeistukset, palveluehdot, toiminnan tarkastusraportit tai sertifioinnit. Siitä kuinka laajasti

esitetään dokumentaatiota, riippuu eri käsittelytoimista ja rekisterinpitäjän riskiarvion laajuudesta. Rekisterinpitäjän suojatoimien riittävyyden arvioinnissa tulee ottaa huomioon käsittelijän asiantuntemus, käsittelijän luotettavuus, käsittelijän käytössä olevat resurssit ja vielä lisäksi käsittelijän maine, joka voi vaikuttaa päätöksentekoon joko positiivisesti tai negatiivisesti. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 342)

Kun käsittelijä on todettu luotettavaksi ja asiantuntevaksi siirrytään seuraavaan tärkeään kohtaan, nimittäin tietojenkäsittelysopimuksen tekemiseen ja allekirjoittamiseen. Tämän pitää olla käsittelijää sitova sopimus ja sen puuttuminen rikkoo asetuksen velvoitteita, josta voi määräytyä seuraamus. Sopimuksessa tulee sopia esimerkiksi salassapitovelvollisuudesta, alikäsittelijöiden laadusta ja myös tiedonkulun toimintatavoista.

3.3.2 Suostumuksen merkitys

Suostumus on ensimmäinen lainmukaisista henkilötietojen käsittelyyn liittyvistä perusteista TSA 6 artiklassa. (Korpisaari;Pitkänen;& Warma-Lehtinen, 2022, s. 145) Se on hyvin tärkeä lainmukainen periaate luotettavassa ja läpinäkyvässä henkilötietojen käsittelyssä. Suostumus tarkoittaa TSA 4 artikla kohta 11 mukaan, ”mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen.” Suostumuksen avulla rekisterinpitäjät voivat käyttää rekisteröidyn henkilötietoja suostumuksen mukaisesti. Rekisterinpitäjällä on kuitenkin monia muitakin velvollisuuksia suostumuksen saamiseen liittyen.

Suostumuksen oikeaoppinen tekeminen on hyvin tärkeää rekisterinpitäjälle, koska sen on pystyttävä osoittamaan rekisteröidyn suostumuksen tietojen käsittelyssä. Rekisterinpitäjän tulee olla hyvin tarkkana suostumusta haaliessaan jonkun muun kirjallisen ilmoituksen yhteydessä, koska rekisteröidyn tulee olla selvästi tietoinen antamastaan suostumuksesta. Toisin

sanoen suostumuksen antamista koskeva pyyntö esitettävä erillään muista asioista ja sitä ei saa piilottaa. TSA 42 kohdan mukaan vähimmäisvaatimukset tietoiseen suostumukseen ovat rekisterinpitäjän henkilöllisyys ja tarkoitus, jota varten henkilötietoja käsitellään, mutta nämäkin voivat vaihdella tapauskohtaisesti.

Rekisteröidyn tulee antaa suostumus vapaaehtoisesti. Tämä tarkoittaa, että rekisteröidyllä tulee olla todellinen vapaan valinnan mahdollisuus, kuin myös mahdollisuus myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa se ilman syytä aiheuttamatta haittaa rekisteröidylle. (TSA:n johdanto 42 kohta) Rekisterinpitäjän on varmistettava, että rekisteröidyn suostumuksen peruessa ei muodostu lisäkuluja tai muitakaan negatiivisia seurauksia.

4 KÄYTÄNTEET JA RATKAISUT

Tässä luvussa käsitellään ja analysoidaan ”Tekoälyn mahdollisuudet ja uhat käsittelyssä”-aiheen ympärillä olevia tutkimuksia ja näistä esiin nousseita selviä trendejä ja käsitteitä. Tutkimuksien nostamat selvät painopisteet esitetään selvästi ja helposti ymmärrettävänä taulukkona, jota analysoidaan ja avataan sanallisesti.

4.1 Tekoälyn mahdollisuudet henkilötietojen käsittelyssä

Alla oleva taulukko on luotu Fulton Richard, Diane Fulton, Nate Hayes ja Susan Kaplan tutkimuksen ”The transformation risk-benefit model of artificial intelligence: balancing risks and benefits through practical solutions and use cases” pohjalta. Taulukkoon on eriteltynä viisi eri osa-aluetta, jotka kuvaavat laajoja kokonaisuuksia yhteiskunnassamme. Esimerkkejä sarakkeeseen on kirjattu kullekin osa-alueelle ominaisia hyötyjä tekoälyn mahdollisista vaikutuksista. Nämä esimerkit ovat suuntaa antavia siitä, mitä

tekoälyratkaisuja voisi kehittää yhteiskuntaamme, jotta siitä tulisi entistä turvallisempi, avoimempi, tehokkaampi ja luotettavampi.

Osa-alueet	Esimerkkejä
Yhteiskunta	Maailmanlaajuinen tehokkuuden kasvu, yhteiskunnallinen hyvinvointi, vaikutus UN asettamiin kestävyystavoitteisiin, kulttuurillisten esteiden selättäminen
Talous	Korkeampi taitoisten ja paremmin maksavien töiden lisääntyminen, kannattavuuden parantuminen ja sijoitetun pääoman tuoton optimisointi
Virkavalta	Syvä väärennöksien tunnistaminen, edistää taistelemaan kyberrikollisuutta ja huijauksia vastaan ja lisää tekoälyn käytön sääntöjä ja uskottavuutta
Tieto	Lisää läpinäkyvyyttä ja toistettavuutta, luo luotettavia ja riittäviä tietopankkeja ja parantaa tietojen integrointia ja jatkuvuutta
Organisaatiot ja yritykset	Parantaa asiakaskokemuksien personointia, lisää ymmärrystä yrityksen tarpeista, parantaa tietojen jakamista ja yhteistyötä

Tässä taulukossa on havaittavissa erilaisia tekoälyratkaisujen mahdollisuuksia eri yhteiskunnan osa-alueilla. Ylimpänä taulukossa on käsitelty yhteiskuntaa yleisesti ja sen tekoälyratkaisujen mahdollisista vaikutuksista. Maailmanlaajuinen tehokkuuden kasvu on mahdollista erilaisten tekoälyratkaisujen esimerkiksi valtion erilaiset hyväksymisprosessit. Taloudessa taas työllisyyden näkymät voivat olla tekoälyn kehittymisen myötä edulliset. Yleisesti ottaen tekoälyn tehdessä yksinkertaisemmat työtehtävät vapautuvat asiantuntijoille enemmän aikaa tietotaitoisempiin tehtäviin. Virkavallalla on mahdollisuus hyötyä tekoälyratkaisuista huomattavasti, joka auttaa rikollisuuden vähentämiseen entisestään. Tieto auttaa monia eri tekoälyratkaisuja ja niihin käytetään nykyään entistä isompia tietopankkeja. Turvallisuuden varmistaminen tällä osa-alueella on hyvin tärkeää erilaisten tietosuojarikkeiden mahdollisuuden takia. Organisaatio ja yritykset ovat tällä hetkellä aallonharjalla tekoälyn käyttöönoton kanssa ja näiden valossa

tekoälyratkaisut parantavat asiakaskokemuksia ja yritysten tehokkuutta yleisesti.

Tässä taulukossa henkilötiedoista ei itsessään puhuttu riittävästi, mutta jokaiseen eri osa-alueeseen kuuluu valtava määrä henkilötietoja, joita yleisen tietosuoja-asetuksen mukaisesti tulee suojella. Yhteiskunnassa jaetaan vaan toiminnalle välttämättömiä henkilötietoja, esimerkiksi organisaatioiden ja yritysten käyttöön, taloudessa vältetään erilaisten syrjäytymisen riskejä ottamalla vaan tarkkaan valitut henkilötiedot, virkavalta käyttää vain rikoksen selvittämiseen välttämättömiä tietoja ja tietopankkien suuruuksia säädellään.

Alla oleva taulukko on luotu Kaushikkumar Patel tutkimuksen ”Ethical reflections on data-centric AI: balancing benefits and risks” pohjalta. Taulukossa on eriteltynä neljään eri osa-alueeseen, joihin tekoälyratkaisut vaikuttavat. Tekoälyratkaisujen soveltamiskohteet ja konkreettiset edut ovat taulukossa tiivistettynä muutamiin avainsanoihin. Nämä osa-alueet ovat valittu opinnäytetyön aihe huomioiden. Jokaisessa osa-alueessa käytetään henkilötietoja, toisissa

Osa-alue	**Soveltamiskohde**	**Konkreettiset edut**
Terveydenala	sairauksien diagnosointi, lääkkeiden tutkinta	parantuneet potilastulokset, kustannussäästöt
Talous	petosten havaitseminen, riskin arviointi	tehostettu turvallisuus, tehokkaat toiminnot
Itseohjautuvat kulkuneuvot	itseohjautuvat autot, liikenteen hallinta	lisääntynyt turvallisuus, ruuhkan vähentäminen
Jälleenmyynti	asiakkaiden suositukset, varaston hallinta	paranneltu asiakaskokemus, lisääntynyt myynti

Tämä taulukko kuvastaa hyvin eri osa-alueiden tekoälyratkaisujen tilasta. Kaikkien osa-alueiden kohdalla tekoäly on tuonut selviä parannuksia toimintaan ja toimintojen päivittämistä varmasti jatketaan tulevaisuudessa. Henkilötietojen käsittely on ominaista jokaiselle osa-alueelle. Taulukossa ylimpänä käsitellään kaikista kriittisimpiä henkilötietoja ja alimpana vähiten kriittisempiä. Nämä asettavat selvät periaatteet ja toimintatavat tekoälyn käytössä.

Terveydenala hyötyy kriittisistä potilastiedoista, joiden tietosuoja tulee olla huippuluokkaa, koska potilastietoihin kuuluvat sairaudet, henkilötunnukset, osoitteet, lähiomaiset ja monia muita yleisen tietosuoja-asetuksen piiriin kuuluvia vahvoja tunnistettavia tietoja. Näistä on erityistä hyötyä terveydenalalla, mutta tekoälyn käyttöönotossa tulee olla erityisen tarkkana, ettei tietosuojan rikkomisen mahdollisuutta synny. Talous hyötyy myös monista vahvoista tunnistettavissa olevista tiedoista, esimerkiksi henkilötunnus, palkkatiedot, osoite, joten tietosuojaa tulee varjella erityisen tarkasti. Taloudessa taulukossa kuvattu riskin arvioinnin tekoälyratkaisu tulee tuottaa sellaisella tavalla, ettei siitä synny vaaraa esimerkiksi syrjinnälle. Itseohjautuvat kulkuneuvot käyttävät pitkälti vahvoja epäsuoria ja epäsuoria tunnisteita, kuten henkilön sijaintitietoja ja puhelimen tietoja. Jälleenmyyntiä ohjaa ihmisten ostokset ja ostotottumukset, joten tämä osa-alue yleisesti käyttää vähiten henkilötietoja, mutta monilla jälleenmyyntiyrityksillä on esimerkiksi kanta-asiakkuusohjelmat, joissa henkilöt jakavat omia tietojansa, kuten nimi, osoite ja joissain tapauksissa jopa henkilötunnuksia.

Kaikille tämän tutkimuksen taulukossa oleville osa-alueille tekoälyratkaisut ovat olleet huomattava etu ja niiden kehittäminen vaan parantaa etujen mahdollisuuksia, mutta osa-alueiden henkilötietojen suojaa tulee entistä paremmin ylläpitää ja kaikkiin tietosuojariskeihin tulee varautua.

4.2 Tekoälyn uhat henkilötietojen käsittelyssä

Tekoäly on mullistanut monien eri yhteiskunnallisesti tärkeiden osa-alueiden toiminnan. Toimintatapoja tehostetaan ja monissa kuluissa säästetään. Vaikka

tekoälyratkaisuissa on paljon hyviä puolia, liittyy siihen myös useita uhkia, joita yritetään hallita säätämällä maakohtaisesti lakeja ja maanosittain esimerkiksi Euroopassa direktiiveillä ja asetuksilla. Tässä luvussa käsitellään tekoälyn uhkien mahdollisuuksia taulukoiden muodossa samoihin tutkimuksiin viitaten kuin luvussa 4.1.

Alla oleva taulukko on luotu Fulton Richard, Diane Fulton, Nate Hayes ja Susan Kaplan tutkimuksen ”The transformation risk-benefit model of artificial intelligence: balancing risks and benefits through practical solutions and use cases” pohjalta. Taulukko on jaettu viiteen osa-alueeseen, joista jokaisesta osa-alueesta otettu esimerkkejä tekoälyratkaisujen mahdollisista uhista.

Osa-alueet	Esimerkkejä
Yhteiskunta	Maailmankriisit, kulttuurilliset esteet, ihmisoikeudet, maiden väliset profiloinnit ja maakohtainen spesifioitu tekoälyn käyttö ja riittämätön tieto tekoälyn arvoista ja eduista
Talous	Korkeat kustannukset asiakkaille, voi aiheuttaa yhteiskunnan polarisoitumista
Virkavalta	Tekijänoikeuskysymykset, sisäänrakennettu puolueellisuus ja mahdollinen syrjinnän vaara, heikentynyt yksityisyys ja tekoälyn aseistaminen haitallisiin tarkoituksiin
Tieto	Tiedon puute tekoälyratkaisujen vahvistamiseksi, tietojen muoto, määrä ja laatu, tiedonkeruustandardien puute
Organisaatiot ja yritykset	Organisaatioiden vastustaminen tietojen jaossa ja yhteistyössä, uhka työvoiman irtisanomiselle ja uudelleenkoulutukselle ja resurssien puute

Tässä taulukossa on tuotu esille yhteiskunnallisesti tärkeät osa-alueet ja niihin mahdolliset tekoälyratkaisujen uhat esimerkkien muodossa. Yhteiskuntaa on yleisesti käsitelty isojen uhkakuvien muodossa esimerkiksi maailmankriisit, ihmisoikeudet ja maiden väliset profiloinnit. Näistä jokainen on toistaan suurempi uhkakuva, joka varmasti vaikuttaa yleiseen näkemykseen

tekoälyratkaisuihin liittyen. Hallitsematon tekoäly voi uhata ihmisoikeuksien toteutumisen, maiden väliset profiloinnit voivat aiheuttaa syrjintää ja nämä yhdessä voivat aiheuttaa jo jonkinlaisen maailmankriisin, jos näitä ei hallita jollain tavalla. Taloudessa voivat erilaiset varallisuuserot kasvaa korkeiden kustannusten muodossa, koska rikkaammat ihmiset saavat uusimpia tekoälyratkaisuja käyttöönsä oman varallisuuden kasvattamiseen. Virkavallan mahdollisina isoina uhkina ovat syrjinnän vaara ja henkilöiden yksityisyyden menettäminen, varsinkin jos valvontaa tehostetaan tekoälyn avulla. Tiedon osa-alueella tiedon puute ja laatu ovat varmasti isoimmat uhat, koska puute ja huonolaatuinen tieto voivat aiheuttaa yhdessä vaarallisia vääristymiä tekoälyratkaisujen tuloksissa. Organisaatioissa ja yrityksissä isoin uhka on työpaikkojen menettämisen mahdollisuus tekoälylle.

Näiden osalta henkilötietojen suojelemisen uhkia ovat selvästi ihmisoikeuksien rikkomiset, syrjinnän mahdollisuus, tiedon puutteellisuus ja viallisuus sekä yksityisyyden menettäminen. Aikaisempaan viitaten yhteiskunnallisesti tärkeisiin osa-alueisiin voidaan välittömästi vaikuttaa laeilla ja erilaisilla asetuksilla.

Taulukko luotu Kaushikkumar Patel tutkimuksen ”Ethical reflections on data-centric AI: balancing benefits and risks” pohjalta. Aikaisempaan taulukkoon poiketen alla oleva taulukko on jaettu kuuteen eri osa-alueeseen, jotka käsittelevät tekoälyn mahdollisia uhkia näille osa-alueille.

Osa-alueet	**Kuvaus**	**Esimerkit tai seuraukset**
Tietosuoja	Henkilötietoihin luvaton pääsy tai niiden käyttö	Tietomurrot, henkilöllisyys varkaudet

Puolueellisuus tiedoissa	Syrjintä tai epäoikeudenmukainen kohtelu datan takia	Epäoikeudenmukaiset palkkaamisen käytännöt, puolueelliset lainan hyväksynnät
Läpinäkyvyys	Selvyyden puute tekoälyn päätöksenteossa	Kyvyttömyys tulkita tekoälyn päätöksiä tai luottamuksen menettäminen
Vastuullisuus	Puutteellinen vastuunkanto tekoälyjärjestelmien tuloksissa	Syyn tai vastuunjaon osoittamisen vaikeus tekoälyn virheissä
Oikeudenmukaisuus	Epäreilu tai puolueellinen tulos eri ryhmille	Syrjivä tekoälyn algoritmi, puolueelliset rikossyytteet
Suostumus	Informoidun suostumuksen puute tietojen tai tekoälysovelluksien käytössä	Luvaton henkilötietojen käyttö, eettiset dilemmat

Tietosuoja itsessään käsittää kaikkia muita alla olevia osa-alueita jollain tavalla. Itse tietosuojasta on nostettu esiin tietomurrot ja henkilöllisyys varkaudet, jotka ovat äärimmäisen suuria riskejä. Pahimmassa tapauksessa henkilöllisyyden varkaudessa henkilöt voivat menettää luottotietonsa varkaiden ostaessa heidän tiedoillaan tavaroita ja palveluita. Puolueellisuus tiedoissa koskee aikaisemmin käsiteltyä syrjintää, eli epäoikeudenmukaiset palkkaamisen käytännöt ja puolueelliset lainan hyväksynnät liittyvät tähän vahvasti. Uhkana palkkauksen syrjinnässä voi olla esimerkiksi tekoälyn lajittelu nimien perusteella tai syrjintä lainan hyväksynnässä esimerkiksi tiettyjen ihmisryhmien suuri lainojen hylkääminen. Läpinäkyvyydessä tekoälyratkaisujen tulkinnan epäselvyys voi johtaa helposti luottamuksen menettämiseen. Vastuullisuudessa on uhkana vastuunkannon puutteellisuus tekoälyratkaisujen virheiden kohdalla. Oikeudenmukaisuus liittyy vahvasti

puolueellisuuteen tiedoissa kohtaan, mutta tähän lisänä esimerkiksi puolueelliset rikossyytteet ovat suurena uhkana. Suostumuksesta isoin uhka on henkilötietojen luvaton käyttö, joka voi huomaamattakin tapahtua henkilölle, jota ei informoida tarpeeksi selvästi henkilötietojen käsittelystä.

Tässä luvussa käsiteltiin kahta tutkimusta ja niiden tärkeimmistä huomioista tekoälyn uhkiin liittyen henkilötietojen käsittelyssä. Esiin nousi monia yleiselle tietosuoja-asetukselle tärkeitä periaatteita, joita valvotaan tarkasti ja sen mukaan noudatetaan poikkeuksetta.

5 YHTEENVETO JA JOHTOPÄÄTÖKSET

Tekoäly on vahvasti osa meidän yhteiskuntaamme ja se on tullut jäädäkseen. Tekoälyn nopean kehittymisen myötä monet henkilötietojen suojaamiseen liittyvät asiat voivat vanhentua ja uusille ratkaisuille on tarvetta. Euroopassa kuitenkin vallitsee kattava asetus, joka takaa yleisen henkilötietosuojan. Tämä ei kuitenkaan kaikkeen henkilötietojen suojaamisen anna suoraa vastausta, vaan liikkumavaraa kuitenkin löytyy. Siitä huolimatta henkilötietojen suojaaminen on ehdoton prioriteetti tekoälyratkaisuja kehittäessä.

Opinnäytetyötä kirjoittaessa olen oppinut laajasti tekoälystä, henkilötietojen suojaamisen perusteista ja yleisestä tietosuoja-asetuksesta. Teoriapohjaa reflektoiden analysoin kahden henkilötietojen käsittelyyn liittyvää tutkimusta ja olin yllättynyt kuinka moneen eri tarkoitukseen ja osa-alueeseen tekoäly nykyään vaikuttaa. Näiden osa-alueiden ansiosta tekoäly tulee olemaan entistä vahvemmin yhteiskunnassamme ja saamme nauttia sen tuomista eduista.

Tekoälyn tulevaisuus on vielä auki, mutta näiden tietojen pohjalta matka on vain ylöspäin. Kaikki toimialat hyötyvät tulevaisuudessa tavalla tai toisella tekoälystä ja näen siinä enemmän potentiaaleja kuin uhkia. Vahvoihin

tunnistettaviin henkilötietoihin on kehitettävä kryptinen pohja, jota tekoäly itsessään ei pysty avaamaan. Tutkimuksen tavoitteena oli muodostaa peruskäsite tekoälylle ja henkilötietojen käsittelylle sekä niihin liittyvien tutkimusten analysointi.

LÄHTEET

Council of Europe. (2024, Toukokuu 9). History of Artificial Intelligence. Retrieved from Council of Europe Artificial Intelligence: https://www.coe.int/en/web/artificial-intelligence/history-of-ai

Ehud Y., S. (1983). The fifth generation project - a trip report. Communications of the ACM.

Euroopan ihmisoikeussopimus 63/1999. (ei pvm). Noudettu osoitteesta https://www.finlex.fi/fi/sopimukset/sopsteksti/1999/19990063/19990063_2

Fulton, R.;Fulton, D.;Hayes, N.;& Kaplan, S. (2024). The transformation risk-benefit model of artificial intelligence: balancing risks and benefits through practical solutions and use cases. IJAIA. Noudettu osoitteesta https://deliverypdf.ssrn.com/delivery.php?ID=942094068073005099087096117089124086034008059068089043102125103104085002073090116076103052038060105029109006067078123127102029052078027028048094121030005080112002029095043064103099124078089006073087022093098019

Järvinen, P. (2023). Tekoäly ja minä : ihmisenä tekoälyn aikakaudella. Tammi.

Kolari, J.;& Kallio, A. (2023). Tekoäly 123 : matkaopas tulevaisuuteen. Docendo.

Korpisaari, P.;Pitkänen, O.;& Warma-Lehtinen, E. (2022). Tietosuoja. Alma Talent Oy 2. uudistettu painos.

Lutkevich, B. (2022, 8). TechTarget. Retrieved from AI winter: https://www.techtarget.com/searchenterpriseai/definition/AI-winter

Metropolia Ammattikorkeakoulu. (18. Toukokuu 2024). Syväoppiminen. Noudettu osoitteesta Tekoälyn perusteet: https://sites.google.com/metropolia.fi/tekoalynperusteet/etusivu/syv%C3%A4oppiminen

OECD. (1980). Guidenlines on the Protection Privacy and Transborder Flows of Personal Data. OECD.

Euroopan Parlamentti. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Euroopan unionin neuvosto. Noudettu osoitteesta https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Patel, K. (2024). Ethical reflections on data-centric ai: balancing benefits and risks. IAEME. Noudettu osoitteesta https://www.researchgate.net/profile/Kaushikkumar-Patel-4/publication/377263257_Ethical_Reflections_on_Data-Centric_AI_Balancing_Benefits_and_Risks/links/659d71bb0bb2c7472b3f02d8/Ethical-Reflections-on-Data-Centric-AI-Balancing-Benefits-and-Risks.pdf

Rudgard, S. (2019). Origins and Development of European Data Protection Law. Teoksessa U. (. Eduardo, European Data Protection: Law and Practice. IAPP Second Edition.

Salo, I. (2023). Luova tekoäly mullistaa kaiken : ChatGPT näyttää tietä. Teoksessa I. Salo, Luova tekoäly mullistaa kaiken : ChatGPT näyttää tietä (s. 17). Helsingin seudun kauppakamari.

SAP SE. (15. Toukokuu 2024). Tekoäly, Mitä koneoppiminen on? Noudettu osoitteesta SAP-sivusto: https://www.sap.com/finland/products/artificial-intelligence/what-is-machine-learning.html

Tableau. (2024, Toukokuu 19). What are the advantages and disadvantages of artificial intelligence (AI)? Retrieved from Tableau: https://www.tableau.com/data-insights/ai/advantages-disadvantages#advantages-and-disadvantages

Tietoarkisto. (24. toukokuu 2024). Tunnisteellisuus ja anonymisointi. Noudettu osoitteesta Tietoarkisto sivusto: https://www.fsd.tuni.fi/fi/palvelut/aineistonhallinta/tunnisteellisuus-ja-anonymisointi/

Tietosuojavaltuutetun toimisto. (30. Toukokuu 2024). Henkilötietojen käsittelyn roolit ja vastuut tieteellisessä tutkimuksessa. Noudettu osoitteesta Tietosuojavaltuutetun toimisto sivustot: https://tietosuoja.fi/henkilotietojen-kasittelyn-roolit-ja-vastuut

Tietosuojavaltuutetun toimisto. (25. toukokuu 2024). Käyttötarkoitussidonnaisuus. Noudettu osoitteesta Tietosuojavaltuutetun toimisto sivustot: https://tietosuoja.fi/kayttotarkoitussidonnaisuus

Tietosuojavaltuutetun toimisto. (25. toukokuu 2024). Lainmukaisuus, asianmukaisuus ja läpinäkyvyys. Noudettu osoitteesta Tietosuojavaltuutetun toimisto sivusto: https://tietosuoja.fi/lainmukaisuus-asianmukaisuus-lapinakyvyys

Tietosuojavaltuutetun toimisto. (25. 05 2024). Luottamuksellisuus ja turvallisuus. Noudettu osoitteesta Tietosuojavaltuutetun sivustot: https://tietosuoja.fi/luottamuksellisuus-ja-turvallisuus

Tietosuojavaltuutetun toimisto. (25. toukokuu 2024). Tietojen minimointi. Noudettu osoitteesta Tietosuojalvaatutetun toimisto sivustot: https://tietosuoja.fi/tietojen-minimointi

Weizenbaum, J. (1966). Computional Linguistics. Communications of the ACM.

Winter, A. (18. Toukokuu 2024). Tekoäly ja neuroverkot. Noudettu osoitteesta Ite Wiki: https://www.itewiki.fi/p/tekoaly-ja-neuroverkot