EU AI ACT – asetuksen vaatimukset organisaatioiden riskienhallintaan

Aaro Tanner

Haaga-Helia ammattikorkeakoulu
Tietojenkäsittely Tradenomi
Opinnäytetyö
2025

Tiivistelmä

Tekijä
Aaro Tanner

Tutkinto
Tradenomi, tietojenkäsittely

Raportin/Opinnäytetyön nimi
EU AI Act – asetuksen vaatimukset organisaatioiden riskienhallintaan

Sivu- ja liitesivumäärä
40

Tutkimuksen tavoitteena oli selvittää ja analysoida, miten Euroopan unionin tekoälysäädöksen keskeiset vaatimukset vaikuttavat erityisesti riskienhallintaan organisaatioissa. Tutkimus toteutettiin laadullisena, kuvailevana kirjallisuuskatsauksena. Tietolähteinä käytettiin lainsäädäntöä, asetuksia, standardeja, internetartikkeleita, tieteellisiä julkaisuja, uutisia, ministeriöiden verkkosivuja sekä muuta aiheeseen soveltuvaa aineistoa. Aineistossa tarkasteltiin kyberturvallisuutta, tekoälyn turvallisuutta sekä sääntelyyn liittyviä näkökulmia. Erityinen painopiste oli EU AI Actin riskiluokittelussa, sääntelyvaatimuksissa ja niiden vaikutuksissa organisaatioiden turvallisuuskäytäntöihin. Tutkimuksessa ei syvennytty teknisiin yksityiskohtiin tai eettisiin kysymyksiin.

EU AI Act on maailman ensimmäinen laajamittainen tekoälyn sääntelykokonaisuus, ja sen käytännön vaikutukset ovat monilta osin vielä hahmottumattomia. Vaikka aiheesta on julkaistu runsaasti tietoa, se on usein hajanaista, teknisluonteista ja juridista, mikä voi tehdä siitä vaikeasti lähestyttävän. Asetus ei ainoastaan ohjaa tekoälyn teknistä kehitystä, vaan myös luo perustaa eettiselle ja oikeudelliselle kehykselle teknologian käytölle. Tämän vuoksi sen tarkastelu käytännönläheisestä näkökulmasta on tärkeää niin organisaatioille kuin koko yhteiskunnalle. Asetus vaikuttaa myös tietoturvallisuuteen, ja sen ymmärtäminen tukee osaamista erityisesti tietoturva-alalla. Tutkimusaihe valittiin sen ajankohtaisuuden, merkityksellisyyden ja yhteiskunnallisen vaikuttavuuden vuoksi. Tulokset tarjoavat käytännön suosituksia organisaatioille, jotka valmistautuvat sääntelyn voimaantuloon.

Tutkimuksessa havaittiin, että EU AI Act asettaa uusia vaatimuksia etenkin korkean riskin tekoälyjärjestelmien osalta, mukaan lukien riskinarviointi, läpinäkyvyys, ihmisen valvonta ja tietoturva. Järjestelmien on myös täytettävä tekniset standardit, ja niistä on pidettävä yksityiskohtaista dokumentaatiota. Organisaatiot voivat sopeutua asetukseen kehittämällä vastuullisen tekoälyn prosesseja, investoimalla riskienhallintaan ja varmistamalla teknisen ja juridisen asiantuntemuksen sekä tuottamalla tarvittavan dokumentaation.

Organisaatiot voivat kohdata haasteita sääntelyn tulkinnassa, teknisten vaatimusten täyttämisessä ja dokumentointivelvoitteiden toteuttamisessa. Resursointi ja kyvykkyydet ovat keskeisessä asemassa. Sääntely nähtiin myös mahdollisuutena: se voi tarjota uusia liiketoimintamalleja ja kilpailuetua toimijoille, jotka panostavat vastuulliseen tekoälyn kehittämiseen.

Asiasanat
EU AI Act, sääntely, kyberturvallisuus, tekoälyjärjestelmä, tekoäly, riskienhallinta

Sisällys

1 Johdanto

Tekoäly (AI) on viime vuosina tullut yhä tärkeämmäksi osaksi arkipäivää ja liiketoimintaa. Monet yritykset hyödyntävät tekoälyä esimerkiksi automatisoiduissa prosesseissa ja päätöksenteossa, mikä tekee AI:stä kriittisen teknologian monilla eri aloilla. Samalla kuitenkin tekoälyyn liittyvät turvallisuuskysymykset ovat nousseet vahvasti esille ja niihin on nyt tartuttu lainsäädännöllä. EU AI Act on Euroopan unionin ensimmäinen laaja-alainen tekoälyn sääntelykehys, joka pyrkii varmistamaan, että tekoälyä käytetään turvallisesti ja eettisesti. Tämä tekee asetuksesta tärkeän, sillä sen sääntelyllä voi olla kauaskantoisia vaikutuksia niin yritysten toimintaan kuin yhteiskunnan turvallisuuteen. Asetuksen tavoitteena on suojella käyttäjiä ja yrityksiä tekoälyyn liittyviltä riskeiltä ja varmistaa, että AI-järjestelmät ovat luotettavia ja vastuullisia.

Tutkimuksessa tarkastellaan EU AI Actia erityisesti sen vaikutusten kautta organisaatioihin. Tekoälyjärjestelmiin liittyy monia riskejä, kuten mahdollisuus väärinkäyttöön, tietoturvauhkien lisääntyminen ja autonomisten järjestelmien epäluotettavuus. Tutkimuksessa selvitetään, miten EU AI Act vaikuttaa organisaatioiden toimintaan ja millaisia toimenpiteitä vaatimusten täyttäminen edellyttää.

Turvallisuus on keskeinen kysymys tekoälyn käytössä ja EU AI Act tuo siihen liittyen merkittäviä uusia vaatimuksia. Tutkimuksen tavoitteena on tutkia näitä vaatimuksia ja selvittää, miten ne vaikuttavat organisaatioihin, jotka tekoälyä kehittävät tai käyttävät tekoälyä. Tekoäly on nopeasti kasvava ala ja sen turvallisuuden varmistaminen on tärkeää sekä yrityksille että yhteiskunnalle. Tutkimustuloksia voivat hyödyntää erityisesti tekoälyä kehittävät organisaatiot, jotka joutuvat ottamaan turvallisuusvaatimukset huomioon, sekä muut organisaatiot, joissa tekoäly on osa toimintaa. Työ voi tarjota konkreettisia näkökulmia siihen, miten organisaatiot voivat valmistautua EU AI Actin asettamiin vaatimuksiin ja hallita turvallisuuteen liittyviä riskejä.

Yhteiskunnan näkökulmasta tämä tutkimus käsittelee tärkeää aihetta, sillä tekoälyn turvallisuus vaikuttaa suoraan siihen, kuinka paljon siihen voidaan luottaa. EU AI Act pyrkii varmistamaan, että tekoälyä käytetään vastuullisesti ja turvallisesti, mikä on edellytys sen laajamittaiselle hyödyntämiselle. Tutkimus tukee osaltaan ymmärrystä siitä, miten sääntely voi edistää tekoälyn vastuullista käyttöä.

1.1 Tutkimuksen tavoite

Tämän tutkimuksen päätavoitteena on selvittää, miten EU AI Act vaikuttaa organisaatioihin, jotka hyödyntävät tekoälyä toiminnassaan ja millaisia vaatimuksia sääntely tuo riskienhallinnan näkökulmasta.

Tutkimusongelma on: Miten EU AI Act vaikuttaa organisaatioihin ja mitä riskienhallintaan liittyviä vaatimuksia sen täytäntöönpano edellyttää?

Tutkimuksen alaongelmat tarkentavat pääongelmaa ja jäsentävät opinnäytetyön sisältöä. Näihin kysymyksiin vastataan työn eri luvuissa tietoperustan ja muun analyysin kautta. Taulukkoon 1 on koottu peittomatriisi, joka havainnollistaa, miten alaongelmat liittyvät työn rakenteeseen ja varmistaa kokonaisuuden loogisen etenemisen.

Taulukko 1. Peittomatriisi

Alaongelmat	**Tietoperusta (luku)**	**Tulokset (luku)**
Mitä vaatimuksia EU AI Act asettaa tekoälyjärjestelmille?	3, 4	5.1
Miten yritykset voivat sopeutua asetuksen vaatimuksiin?	3.5, 4	5.2, 5.3, 5.4
Millaisia haasteita organisaatiot kohtaavat säätelyn käytännön toteutuksessa?	3.2, 4.2, 4.6	5.5

Työ ei syvenny teknisiin yksityiskohtiin tai eettisiin kysymyksiin, vaan tarkastelee käytännön toimenpiteitä riskienhallinnan näkökulmasta.

Työssäni pyrin edistämään tekoälyn vastuullista käyttöä tuomalla esille konkreettisia keinoja turvallisuusvaatimusten täyttämiseksi. EU AI Actin tavoitteena on suojella käyttäjiä ja yhteiskuntaa tekoälyjärjestelmien riskeiltä ja tämä tutkimus tukee näitä tavoitteita tarjoamalla käytännönläheistä tietoa, joka voi hyödyttää sekä yrityksiä että sääntelyn kehittämistä.

1.2 Tietoperustana kuvaileva kirjallisuuskatsaus

Työ on pääosin laadullinen eli kvalitatiivinen tutkimus, sillä sen tavoitteena on ymmärtää ja analysoida EU AI Actin vaatimuksia sekä niiden merkitystä yrityksille. Tarkastelen aineistoa tapaustutkimuksen ja asiantuntija-analyysien kautta. Tutkimus koostetaan kuvailevana kirjallisuuskatsauksena. Tietoperusta rajataan uusimpiin ja ajankohtaisiin tietoihin. Kirjallisuuskatsaus on menetelmä, jonka avulla kerätään tietoa tutkimuskysymyksiä koskevista aihepiireistä.

Tietoperustassa keskityn tekoälyn turvallisuuteen ja EU AI Actin sääntelyyn liittyviin teemoihin. Työn tietoperusta rakentuu seuraavista keskeisistä teemoista:

1.Tekoälyn turvallisuus:

> Tarkastelen, mitä vaatimuksia EU AI Act asettaa tekoälyjärjestelmien turvallisuudelle ja millaisia toimia organisaatioilta edellytetään.

2.EU AI Actin turvallisuusvaatimukset:

> Analysoin, mitä vaatimuksia EU AI Act asettaa tekoälyjärjestelmien turvallisuudelle ja miten niitä voidaan soveltaa organisaatiotasolla riskienhallinnan näkökulmasta.

3.Riskiluokitus ja yritysten velvoitteet:

> Selvitän, miten EU AI Act luokittelee tekoälyjärjestelmät riskien perusteella ja millaisia vaatimuksia tämä tuo organisaatioille, jotka kehittävät tai käyttävät tekoälyä.

1.3 Aineiston keruu ja tutkimuksen rakenne

Tutkielma on narratiivinen kirjallisuuskatsaus, ja tutkimuksen teoreettinen viitekehys tulee menetelmän mukaisesti erilaisista kirjallisista lähteistä. Lähteet käsittelevät tutkimuksessa määriteltyjä kysymyksiä ja tietolähteinä toimivat lainsäädäntö, asetukset, standardit, internettiartikkelit, tieteelliset artikkelit, uutiset, ministeriöiden sivut sekä muut aiheeseen soveltuva aineisto.

Aineistoja etsittiin muun muassa Haaga-Helian materiaalipankista Google Scholarista, erilaisten artikkeleiden pohjalta, uutispalveluista sekä yritysten ja ministeriöiden verkkosivuilta. Euroopan komission julkaisut ja itse asetus toimivat myös keskeisinä lähteinä. Hakusanoina käytettiin tutkimuskysymyksen mukaisesti esimerkiksi seuraavia termejä: EU AI ACT, EU AI.

Tietohaku toteutettiin sekä suomen- että englanninkielisillä hakutermeillä, jotta mukaan saataisiin mahdollisimman laajasti myös kansainvälistä aineistoa. Hakuprosessissa keskityttiin ensisijaisesti tieteellisiin ja vertaisarvioituihin lähteisiin, mutta tekoälysääntelyyn liittyvän EU AI Act -lainsäädännön ajankohtaisuuden ja tietopohjan hajanaisuuden vuoksi mukaan otettiin myös muita harkinnanvaraisia digitaalisesti saatavilla olevia julkaisuja. Näitä olivat muun muassa viranomaistahojen ja elinkeinoelämän tuottamat materiaalit, joiden sisältöä arvioitiin kriittisesti suhteessa tutkittuun tietoon.

1.4 Keskeiset käsitteet

Taulukossa 2 on esitetty tässä opinnäytetyössä käytettyjä keskeisiä käsitteitä.

Taulukko 2. Keskeiset käsitteet

Sana	Selitys
Algoritmi	Ohjeiden sarja, jota tietokone seuraa ongelman ratkaisemiseksi tai tehtävän suorittamiseksi. (Parviainen 2024)
Big Data	Valtavat tietomassat, joita käsitellään ja analysoidaan tekoälyn avulla löytääkseen piilotettuja kuvoita ja suuntauksia. (Parviainen 2024)
Data-analytiikka	Prosessi, jossa tietoja tutkitaan ja analysoidaan, jotta voidaan tehdä päätelmiä ja ennusteita. (Parviainen 2024)
EU AI Act	EU Artificial Intelligence Act Euroopan unionin asetus, joka säätelee tekoälyn käyttöä ja riskiperusteista valvontaa. (Euroopan parlamentti 2020)
GDPR	General Data Protection Regulation – Euroopan unionin asetus, joka säätelee henkilötietojen keräämistä, käsittelyä ja luovuttamista sekä parantaa yksilöiden tietosuojaa. (Euroopan unioni 2024)
Koneoppiminen	Tekoälyn osa-alue, jossa tietokoneohjelmat oppivat kokemuksesta ja parantavat suorituskykyään ilman eksplisiittistä ohjelmointia. (Parviainen 2024)
Korkean riskin tekoälyjärjestelmä	EU AI Actin määrittelemä tekoälyjärjestelmä, joka vaatii tiukempaa sääntelyä esimerkiksi terveydenhuollon ja työnhaun yhteydessä. (Euroopan parlamentti 2023)
Kyberturvallisuus	Tekoälyjärjestelmän suojautumiskyky tietoturvahyökkäyksiä ja manipulointia vastaan. (Suomen kyberturvallisuusstrategia 2024)
Riskienhallinta	Prosessi, jossa tunnistetaan, arvioidaan ja hallitaan organisaation kohtaamia riskejä, jotta niiden vaikutuksia voidaan vähentää tai estää. (ISO 2018)

Riskiluokitus	EU AI Actin käyttämä malli, joka jakaa tekoälyjärjestelmät eri riskiluokkiin ja määrittelee kullekin luokalle sovellettavat vaatimukset. (Euroopan parlamentti 2020)
Tekoäly	Koneen kyky käyttää ihmisen älyn taitoja, kuten päättelyä, oppimista, suunnittelua ja luomista, ympäristön havainnointiin ja ongelmien ratkaisuun. (Euroopan parlamentti 2020)
Tekoälyn turvallisuus	Tekoälyjärjestelmän kyky toimia ennakoidusti ja ilman, että se aiheuttaa vahinkoa käyttäjille tai ympäristölle. (Euroopan parlamentti 2023)
Tekoälyjärjestelmä	Konepohjainen järjestelmä, joka toimii vaihtelevalla autonomian tasolla ja tuottaa sisältöä, suosituksia tai päätöksiä. (Data Protection Authority of Belgium 2024)
Älykäs agentti	Ohjelma, joka toimii itsenäisesti ja tekee päätöksiä ympäristönsä perusteella. (Parviainen 2024)

2 Kyberturvallisuuden muuttunut turvallisuustilanne

Viimevuosien teknologinen murros ja digitalisaatio ovat luoneet suuria muutoksia turvallisuustilanteessa, erityisesti kyberturvallisuuden saralla. Internettiin kytkettyjen laitteiden määrä sekä teknologiat, kuten tekoäly, ovat luoneet uusia haavoittuvuuksia. Tekoälyn nopea kehitys on lisännyt kyberuhkien monimutkaisuutta, ja sen hyödyntäminen kohdennetuissa ja tehokkaammissa hyökkäyksissä on ollut kasvava trendi. AI:n kehittyminen tuo positiivisia sekä negatiivisia muutoksia normaaliin liiketoimintaan mutta se lisää myös organisaatioille uusia turvallisuusuhkia. Tekoäly voi oppia käyttämään heikkoja kohtia järjestelmissä hyväkseen, jolloin rikollinen käyttö voi olla entistä vaikeampi havaita tai ennakoida. Turvallisuusasiantuntijoilta odotetaan entistä parempaa AI-turvallisuuden ymmärrystä, koska ilman riittäviä turvatoimia tai sääntelyä AI voi aiheuttaa merkittävää vahinkoa yksilöille, yhteiskunnalle sekä yrityksille. (Suomen kyberturvallisuusstrategia 2024.)

Tekoälyn turvallisuuden kehittäminen vaatii ennakoivaa lähestymistapaa sekä jatkuvaa tehostettua valvontaa, koska perinteiset turvatoimet eivät ole enää riittäviä. Vaikka tekoäly parantaa organisaation kyberhyökkäysten torjuntaa ja mahdollistaa edistyneempiä suojausmekanismeja se altistaa organisaation samalla entistä kehittyneemmille hyökkäyksille. Tämän takia on elintärkeää kehittää tekoäly kentälle pelisääntöjä ja sääntelykehyksiä, joilla mahdollistetaan turvallinen teknologian kehitys. (Suomen kyberturvallisuusstrategia 2024.)

Suomi on asettanut tavoitteekseen olla edelläkävijä teknologioiden hyödyntämisessä. Tämä tavoite asettaa vaatimuksia koko elinkaaren hallinnalle. Tekoälyn turvallinen käyttö edellyttää vahvaa osaamista ja syvällistä ymmärrystä, jotta mahdolliset riskit voidaan ennakoida ja omia suojamekanismeja kehittää jatkuvasti. Tekoäly voi myös aiheuttaa merkittäviä seurauksia, kuten tietovuotoja, tekoälyhyökkäyksiä ja muita kyberuhkia, jotka voivat pahimmillaan lamauttaa yhteiskunnan keskeisiä toimintoja. (Suomen kyberturvallisuusstrategia 2024.)

Valitettavasti korkean teknologian kehitys tuo mukanaan myös suurempia hyötyjä kyberrikollisuudelle. Kyberrikollisuus on muuttunut yhä kohdennetummaksi ja tehokkaammaksi, ja sen torjunta edellyttää jatkuvia ja aktiivisia toimenpiteitä kaikilta organisaatioilta. Elämme maailmassa, joka on jatkuvan muutoksen tilassa, mikä tekee varautumisesta entistä tärkeämpää. Kyberrikollisuuden ennaltaehkäisy vaatii lainsäädännön sekä kansallisten turvallisuusstrategioiden jatkuvaa kehittämistä. Viranomaisten, yritysten ja kansalaisten välinen yhteistyö on avainasemassa, jotta kyberuhkia voidaan torjua tehokkaasti ja vahvistaa koko yhteiskunnan vastustuskykyä. (Suomen kyberturvallisuusstrategia 2024.)

Kyberturvallisuuden varautuminen Suomessa on monivaiheinen ja monimutkainen prosessi, jossa on otettava huomioon lainsäädäntö, viranomaiset, teknologiset ratkaisut ja organisaatioiden kyvykkyydet (katso kuva 1). Suomessa toimivat organisaatiot, jotka käsittelevät henkilötietoja, ovat velvollisia huolehtimaan tietoturvasta tietosuojalainsäädännön mukaisesti. Tämä tarkoittaa, että yritykset ja julkisen sektorin toimijat toteuttavat asianmukaiset tekniset ja organisatoriset toimenpiteet suojatakseen henkilötiedot kyberuhkilta. Henkilötietojen vuotamisesta on ilmoitettava Tietosuojavaltuutetulle, joka valvoo sääntöjen noudattamista. AI voi myös auttaa luomaan ja ylläpitämään ajankohtaista kyberturvallisuuden tilannekuvaa. Tekoäly kykenee käsittelemään suuria tietomassoja tehokkaasti ja tuottamaan tarkempia ennusteita uhkista ja häiriöistä, parantaen näin viranomaisten ja elinkeinoelämän reagointikykyä. AI voi automaattisesti tunnistaa ja estää kyberhyökkäyksiä, kuten haittaohjelmia tai tietomurtoja, reaaliajassa. (Valtioneuvosto 2025.)

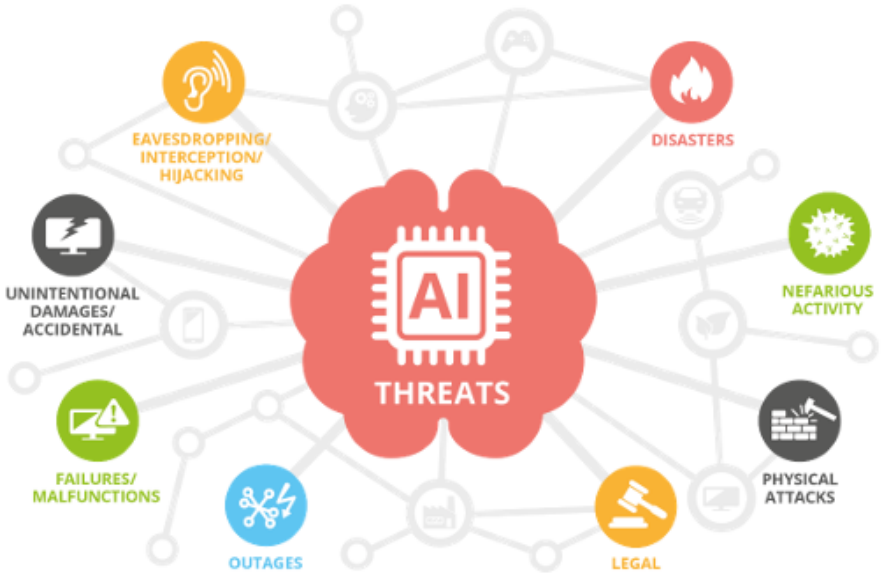
Kuva 1. Kyberturvallisuuden varautuminen

Haasteita, luo se että, AI-järjestelmien on oltava luotettavia, koska virheelliset päätökset voivat johtaa suuriin vahinkoihin. Tekoälyn avulla voidaan myös altistua uusille uhille, kuten mm. adversial attack-hyökkäys, jossa tekijä manipuloi tekoälyn toimintoja hyökkäys tarkoituksiin. Tämän takia kyberturvallisuus on tärkeässä roolissa tekoälyn käytössä ja organisaatioiden järjestelmien täytyy olla riittävän suojattuja ja vahvoja. (Valtioneuvosto 2025.)

Suomi on edelläkävijänä tekoälyn käytössä pohjoismaissa. Tekoälyn hyödyntäminen organisaatioissa on yleistynyt kovaa vauhtia. Suomessa 61 % organisaatioista käyttää tekoälyä ja suuri osa organisaatioista aikoo lisätä tekoälyn käyttöä lähivuosina. Tekoälyä hyödynnetään prosessin automatisointiin ja tuotteiden ja palveluiden laadun parantamiseen. Kuitenkin puolet pohjoismaisista organisaatioista ei käytä tekoälyä lainkaan. Epävarmuus ja tiedonpuute, puutteet digitaalisessa osaamisessa sekä strategian puute tekoälyn kehittämiseen hidastavat organisaatioiden integroitumista tekoälypohjaisiin järjestelmiin. (Microsoft 2024.)

Tekoäly tuo mukanaan monia hyötyjä, kuten prosessien automatisoinnin ja päätöksenteon tehostamisen, mutta se tuo myös merkittäviä kyberturvallisuusuhkia. Tekoälyjärjestelmiin kohdistuvat uhat voivat tulla monilta eri toimijoilta, kuten kyberrikollisilta, valtiollisilta toimijoilta, hacktivisteilta tai jopa kilpailijoilta. Kyberrikolliset voivat käyttää tekoälyä taloudellisten hyökkäysten, kuten tietojen varastamisen tai kiristyshyökkäysten toteuttamiseen. Valtioiden tukemat toimijat voivat puolestaan etsiä haavoittuvuuksia tekoälyjärjestelmistä, joita voidaan käyttää tiedustelutarkoituksiin tai kyberhyökkäyksille. Lisäksi yrityksen sisäiset toimijat voivat tahattomasti tai tahallisesti vahingoittaa tekoälyn koulutusdataa mikä voi vaarantaa järjestelmän toimivuuden. (Enisa 2020.)

Tekoälyjärjestelmien suojaaminen vaatii systemaattista uhkamallintamista, jossa tunnistetaan uhkat, arvioidaan niiden merkitys ja kehitetään suojausstrategioita. Tällöin keskeistä on määrittää järjestelmän suojausominaisuudet, kuten luottamuksellisuus, eheys ja saatavuus, mutta myös tekoälyyn liittyvät erityispiirteet, kuten läpinäkyvyys, selitettävyys ja kestävyys. Uhkamallintaminen seuraa useita vaiheita, kuten tavoitteiden tunnistamista, kriittisten resurssien kartoitusta ja haavoittuvuuksien analysointia. Näiden analyysien avulla voidaan luoda turvallisuusratkaisuja, jotka kohdistuvat erityisesti tekoälyn ainutlaatuisiin uhkiin. (Enisa 2020.)



Kuva 2. Tekoälyuhkien taksonomia (Enisa 2020)

Tekoälyn uhkakenttä voidaan luokitella moniin eri kategorioihin, kuten vahingolliseen toimintaan, salakuunteluun tai fyysisiin hyökkäyksiin. Kuvassa 2 on esitetty tekoälyuhkien taksonomia. Näitä uhkia voidaan tarkastella järjestelmän elinkaaren eri vaiheissa ja ne voivat ilmetä sekä tahattomista että tahallisista toimista. Tekoälyn haavoittuvuudet voivat liittyä myös laajempiin ekosysteemeihin,

kuten pilvipalveluihin tai tietoliikenneverkkoihin. Enisan AI-kyberturvallisuus raportissa tunnistetaan 74 erilaista uhkaa, jotka voivat vaarantaa tekoälyn luotettavuuden ja turvallisuuden. (Enisa 2020.)

Tekoälyn merkitys yhteiskunnassa on valtava ja sen kyberturvallisuuden varmistaminen on elintärkeää, jotta tekoälyjärjestelmät voivat olla luotettavia, turvallisia ja kestäviä. Tekoälyn uhkakenttä paljastaa useita haasteita, kuten monimutkaisuuden, tekniset ongelmat ja tietoturvariskit, jotka vaativat erityistä huomiota. Erityisesti tekoälyyn kohdistuvien uhkien arviointi ja riskienhallinta tulee tehdä ottaen huomioon eri sektoreiden tarpeet ja erityispiirteet. (Enisa 2020.)

3 EU AI ACT

Artificial Intelligence Act on Euroopan unionin uusi tekoälyasetus (EU AI Act 2024/1689), ja se on maailman ensimmäinen tekoälyä kattavasti käsittelevä sääntelykokonaisuus. Tämä kattaa tekoälyn kehittämisestä julkaisuun sekä tämän jälkeiseen käyttöön koskevia velvollisuuksia. Lain tehtävänä on antaa raamit tekoälyyn liittyvälle lainsäädännölle sekä varmistaa tekoälyn läpinäkyvyys ja järjestelmin valvonta. (Euroopan unioni 2024.)

Säädös koskee EU:ssa kehitettyä ja käytettyä tekoälyä, jonka täytyy täyttää vaatimukset luotettavuuden ja perusoikeuksien suojelun osalta. Asetuksen avulla tekoälyn sisämarkkinat ovat EU:ssa yhdenmukaiset, ja se kannustaa teknologian käyttöönottoon, innovointiin sekä kustannusten alentamiseen. (Euroopan komissio 2024.)

Euroopan unionin tekoälyasetus toimii oikeudellisena kehyksenä tekoälyn sääntelylle. Asetus luokittelee tekoälyjärjestelmät riskitason mukaan ja asettaa tiukat vaatimukset erityisesti korkean riskin sovelluksille, kuten terveydenhuollon ja oikeuslaitoksen järjestelmille. Tämä sääntely muuttaa ohjelmistoyritysten liiketoimintamalleja ja kehitysprosesseja sekä lisää vaatimuksia läpinäkyvyydestä, riskinarvioinnista ja ihmisen valvonnasta. EU:n tekoälyasetus korostaa eettisesti kestäviä ratkaisuja ja kehitystä tekoälyn parissa, ja vahvistaa näin eurooppalaisen toimijoiden asemaa globaalisti. Päätarkoituksena on säännellä tekoälyä riskiperusteisella lähestymistavalla sen mukaisesti, miten se kykenee aiheuttamaan vahinkoa yhteiskunnalle: mitä suurempi riski, sitä tiukemmat säännöt. (Ratko 2025.)

Tekoälyasetus vastaa kasvaviin haasteisiin, jotka liittyvät muun muassa perusoikeuksiin, yksityisyyteen ja turvallisuuteen, erityisesti kriittisillä aloilla kuten terveydenhuollossa, oikeusjärjestelmässä ja koulutuksessa. (Ratko 2025).

3.1 Euroopan parlamentin tavoitteet

Euroopan parlamentti painottaa, että tekoälyn käyttö Euroopan unionissa edellyttää korkeita vaatimuksia turvallisuuden, avoimuuden, seurattavuuden ja syrjimättömyyden suhteen. Lisäksi järjestelmien on toimittava sosiaalisesti ja ekologisesti kestävällä tavalla. Tärkeänä pidetään myös sitä, että ihmiset säilyttävät ohjausvastuun tekoälyn toiminnoista automaattisten prosessien sijaan, jotta mahdolliset haitat voidaan ennaltaehkäistä. (Piachqaud-Moustakis 2023.)

Tekoäly nähdään ohjelmistona, joka kykenee saavuttamaan tiettyjä tavoitteita esimerkiksi tuottamalla päätelmiä, sisältöä tai suosituksia, joilla on vaikutusta toimintaympäristöönsä. Huomio kohdistuu erityisesti tekoälyn aikaansaamiin lopputuloksiin ja tavoitteisiin eikä niinkään sen toteutustekniikkaan. (Piac-hqaud-Moustakis 2023.)

Lisäksi parlamentti on tuonut keskusteluun tekoälyn vaikutukset immateriaalioikeuksiin, kuten patenttien ja luovan työn omistajuuden kysymyksiin tilanteissa, joissa tuotokset ovat syntyneet ilman ihmisen suoraa panosta, täysin tekoälyn tuottamina. (Piachqaud-Moustakis 2023.)

Euroopan unioni pyrkii EU AI Act -asetuksella varmistamaan, että tekoälyn kehitys ja käyttö ovat vastuullisia ja eettisesti kestäviä. Tekoälyn odotetaan mullistavan useita toimialoja tehostamalla tuotantoa sekä parantamalla liikenteen turvallisuutta ja tehokkuutta. EU kuitenkin haluaa luoda raamit tekoälyjärjestelmille, jotta eri järjestelmät voidaan luokitella riskiperusteisesti. Tämä auttaa arvioimaan kuinka paljon säätelyä tarvitaan kunkin tason riskiryhmille. EU:n tarkoituksena on luoda turvallisia, läpinäkyviä, jäljitettäviä sekä tasa-arvioisia tietojärjestelmiä. Tämä tuo velvoitteita tekoälyjärjestelmien valmistajille ja käyttäjille sekä korostaa riskienarvioinnin merkitystä. (Euroopan parlamentti 2023.)

3.2 Miksi tekoälylle tarvitaan sääntöjä

Tekoälylaki vahvistaa eurooppalaisten luottamusta tekoälyyn ja sen hallintaan. Vaikka suurin osa tekoälyjärjestelmistä ei aiheuta merkittäviä riskejä ja voi auttaa ratkaisemaan monia yhteiskunnallisia ongelmia, tietyt järjestelmät voivat kuitenkin luoda vaaroja. Näitä on tarpeen huomioida, jotta vältetään haitalliset seuraukset. (Euroopan komissio 2025.)

Voi olla vaikea selvittää, miksi tekoäly on tehnyt tietyn päätöksen tai ennusteen ja ryhtynyt tiettyihin toimiin. Tämä voi estää arvioimasta, onko joku joutunut kohtuuttomasti syrjityksi, esimerkiksi työpaikkahakemuksessa tai julkisten etuuksien hakemisessa. Vaikka olemassa oleva lainsäädäntö tarjoaa osittain suojaa, se ei ole riittävä kohtaamaan niitä erityisiä haasteita, joita tekoälyjärjestelmät voivat tuoda mukanaan. (Euroopan komissio 2025.)

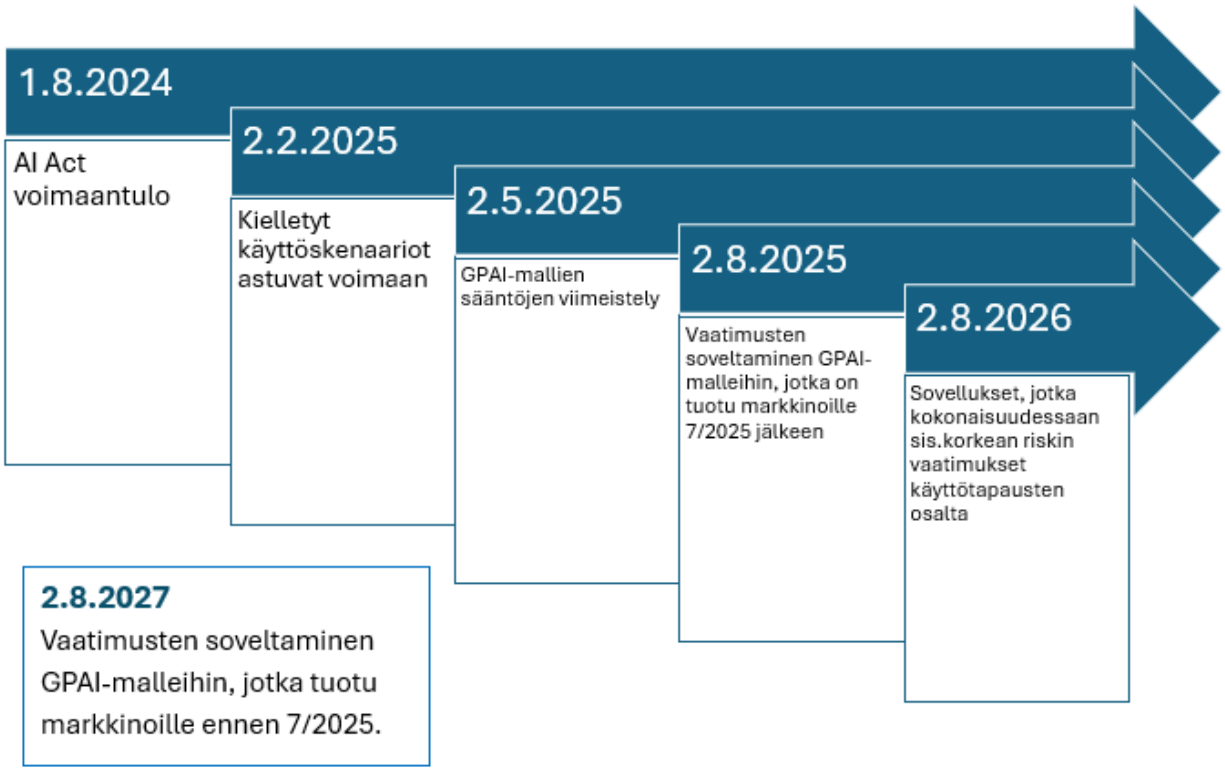
3.3 Aikajana

Parlamentti hyväksyi tekoälysäädöksen maaliskuussa 2024 ja neuvosto puolestaan hyväksyi sen toukokuussa 2024. Lakia aletaan soveltamaan 24 kuukautta sen voimaan astumisen jälkeen. Osaa säännöistä tulee soveltaa heti, erityisesti tekoälyjärjestelmiin, joiden riskiä ei voi hyväksyä. (Euroopan parlamentti 2023.)

Asetus julkaistiin virallisesti 12. heinäkuuta ja astui voimaan 1. elokuuta 2024. Suurin osa sen säännöksistä tulee kuitenkin voimaan vasta 2. elokuuta 2026 (Ratko 2025).

Yleiskäyttöiset tekoälymallit eli GPAI pystyvät suorittamaan laajan kirjon tehtäviä ja muodostavat yhä useammin perustan monille tekoälyjärjestelmille EU:ssa. Laaja-alaisiin tehtäviin kykenevät yleiskäyttöiset tekoälymallit (GPAI) muodostavat yhä useammin tekoälyjärjestelmien teknisen

perustan EU:ssa. Joidenkin mallien merkittävä suorituskyky tai laaja levinneisyys voi aiheuttaa huomattavia yhteiskunnallisia riskejä. Näiden mahdollisten vaikutusten hallitsemiseksi EU:n tekoälyasetus tuo mallien kehittäjille velvollisuuksia, jotka liittyvät muun muassa toiminnan läpinäkyvyyteen ja tekijänoikeuslainsäädännön kunnioittamiseen. (Euroopan komissio 2025.)



Kuva 3. EU AI ACT Täytäntöönpanon aikataulu

Korkean riskin järjestelmillä sääntöä sovelletaan 23 kuukauden kuluttua lain voimaantulosta. Eli näillä järjestelmillä on enemmän aikaa noudattaa lain vaatimuksia (Euroopan parlamentti 2023). Kuvassa 3 on esitelty asetuksen aikajanaa.

- 2.2.2025: EU:n tekoälyasetus astuu voimaan ja kieltää tietyt tekoälykäytännöt, kuten tekoälyn käytön rikollisuuden ennustamiseen persoonallisuusominaisuuksien perusteella, tunteiden tunnistamiseen oppilaitoksissa tai työpaikoilla sekä manipuloivien tai harhaanjohtavien tarkoitusten käyttöön (Työ- ja elinkeinoministeriö 2025).
- 2.8.2025: Suomen ja muiden EU-maiden on nimettävä kansalliset toimivaltaiset viranomaiset, jotka valvovat asetuksen täytäntöönpanoa. Lisäksi on säädettävä seuraamuksista, jotka määräytyvät asetuksen rikkomisesta (Työ- ja elinkeinoministeriö 2025).

- Huhtikuu 2025: Hallitus on esittänyt ensimmäisen vaiheen lainsäädännön eduskunnalle. Tämä koskee kansallisia sääntöjä, jotka liittyvät markkinavalvontaan ja seuraamuksiin asetuksen rikkomisesta (Työ- ja elinkeinoministeriö 2025).
- Kevät 2025: Toisen vaiheen lainsäädännön luonnos, joka koskee muun muassa kansallisten testausympäristöjen (hiekkalaatikko) perustamista ja suuririskisten tekoälyjärjestelmien sääntelyä kriittisessä infrastruktuurissa, on lausuntokierroksella (Työ- ja elinkeinoministeriö 2025).
- Syksy 2025: Hallituksen esitys toisen vaiheen lainsäädännöstä annetaan eduskunnalle ja käynnistetään erillinen toimeenpanoprojekti tekoälyn sääntelyn testausympäristön perustamiseksi (Työ- ja elinkeinoministeriö 2025).

Tekoälyasetuksen päämääränä on varmistaa, että markkinoille tulevat tekoälyjärjestelmät eivät vaaranna ihmisten turvallisuutta, terveyttä tai perusoikeuksia. Se luo myös yhtenäiset säännöt tekoälyjärjestelmien käytölle EU:ssa (Työ- ja elinkeinoministeriö 2025).

3.4 Velvoitteet ja seuraamukset

Asetus koskee kaikkia tekoälyekosysteemin toimijoita. Näitä on esimerkiksi kuvassa 4 olevat EU:n markkinoilla toimivat: toimittajat, käyttäjät, maahantuottajat, jakelijat ja valmistajat. Lisäksi EU:n ulkopuolella kehitetyt, mutta EU:ssa toimivat tekoälyjärjestelmät kuuluvat sääntelyn piiriin. (Ratko 2025).

Kuva 4. Tekoälyekosysteemin toimijat

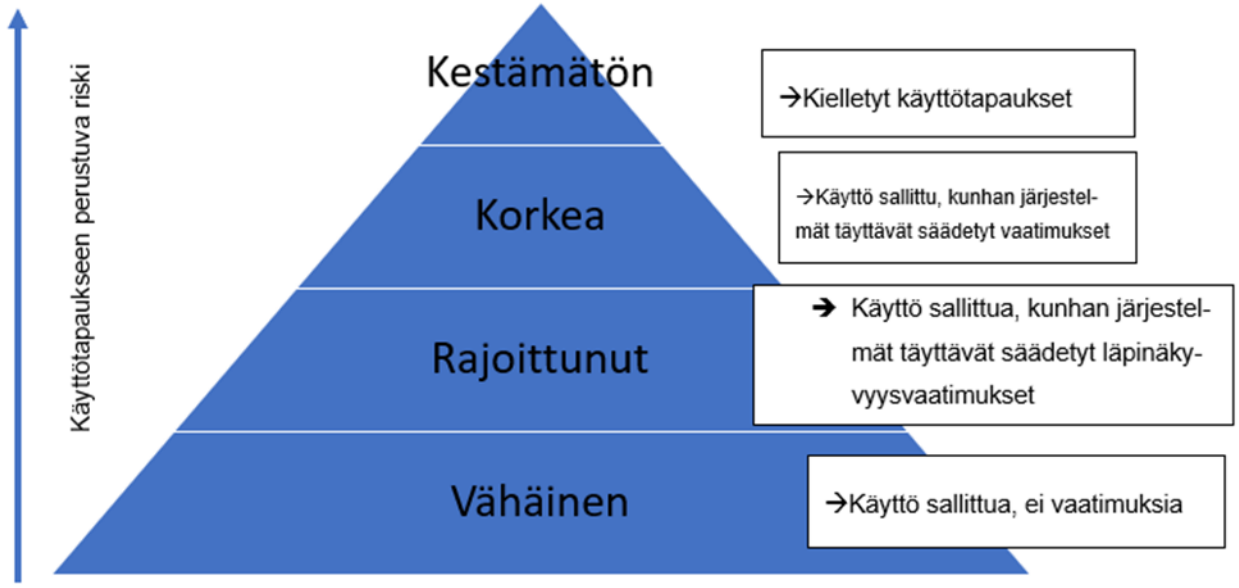
Sääntelyn laiminlyönnistä voi aiheutua huomattavia taloudellisia seuraamuksia. Pienemmissä rikkomuksissa seuraamus voi olla enintään 7,5 miljoonaa euroa tai 1,5 prosenttia yrityksen vuotuisesta maailmanlaajuisesta liikevaihdosta. Vakavammista rikkomuksista seuraamus voi nousta jopa

35 miljoonaan euroon tai 7 prosenttiin vuosiliikevaihdosta, riippuen kumpi on suurempi. (Ratko 2025.)

3.5 Riskiluokittelu

Tekoälysäädöksen riskiperusteisuus jakautuu neljään pääasialliseen riskitasoon, jotka on kuvattu kuvassa 5. Ensimmäinen on kestämätön riski, jota organisaatio ei voi hyväksyä. Tämä tarkoittaa, että tämän tason tekoälyjärjestelmiä ei voida käyttää lainkaan, vaan niiden käyttö kielletään. Kun riski on kestämätön, sen katsotaan rikkovan EU:n arvoja perusoikeuksien näkökulmasta. Seuraavana on korkean riskin taso, jossa riski on suuri tai sen vaikutus voi olla merkittävä turvallisuuteen tai perusoikeuksiin. Tällöin järjestelmä vaatii lisäsääntelyä. Kolmantena on rajoitettu riski, jossa järjestelmille asetetaan läpinäkyvyysvaatimuksia. Alimmalla tasolla ovat vähäisen riskin järjestelmät, joihin suurin osa tekoälyratkaisuista kuuluu.

(Euroopan parlamentti ja neuvosto 2024.)



Kuva 5. Riskiin perustuvat säännökset tekoälyjärjestelmille

Kaikille riskitasoille on määritelty omat vaatimuksensa. Mitä suuremmasta riskistä on kyse, sitä enemmän huomiota järjestelmään tulee kiinnittää, ja sitä tiukemmat vaatimukset siihen kohdistuvat. Korkean riskin järjestelmiin sisältyy pakollinen perusoikeusvaikutusten arviointi (Deloitte 2023).

Perusoikeusvaikutuksen arviointi tarkoittaa sitä, että tarkastellaan, miten jokin ehdotettu säädös tai politiikkatoimi vaikuttaa ihmisten ja ihmisryhmien perus- ja ihmisoikeuksien toteutumiseen. Tämä arviointi tuo oikeudelliset velvoitteet käytännön tasolle ja analysoi, miten esityksen vaikutukset näkyvät ihmisten jokapäiväisessä elämässä. Korkean riskinjärjestelmien kohdalla tämä arviointi on

erityisen tärkeä, koska niillä voi olla merkittäviä vaikutuksia kansalaisten oikeuksiin ja asemaan yhteiskunnassa. Arvioinnissa voidaan esimerkiksi tarkastella, rajoittaako järjestelmä perusoikeuksia, kuten yksityisyyttä, sananvapautta tai syrjimättömyyttä ja miten mahdolliset haittavaikutukset voidaan minimoida. (Oikeusministeriö 2022.)

EU:n kansalaisilla on oikeus tehdä valituksia sekä pyytää selvityksiä heidän oikeuksistaan. Tämä asettaa organisaatioille vaatimuksia: niiden täytyy pystyä tarkistamaan ja selventämään päätösten perusteet alkuperäisestä datasta. (Deloitte 2023.)

3.5.1 Vähäinen ja rajoittunut riskin tekoälyjärjestelmät

Tekoälyasetus ei koske niitä järjestelmiä, joita pidetään vähäisenä tai olemattomana riskiluokituksena. Suurin osa EU:ssa olevista tekoälyjärjestelmistä kuuluvat juuri tähän luokkaan. Esimerkkejä näistä ovat tekoälyä hyödyntävät videopelit ja roskapostisuodattimet. (Euroopan komissio 2025.)

Rajoitetun riskin järjestelmissä sovelletaan avoimuusvaatimuksia. Organisaatioille voi tulla tiedonantovelvoitteita, jotta käyttäjät tietävät, milloin tekoälyä käytetään ja voivat näin hyväksyä tai kieltäytyä sen käytöstä. (Euroopan komissio 2025.)

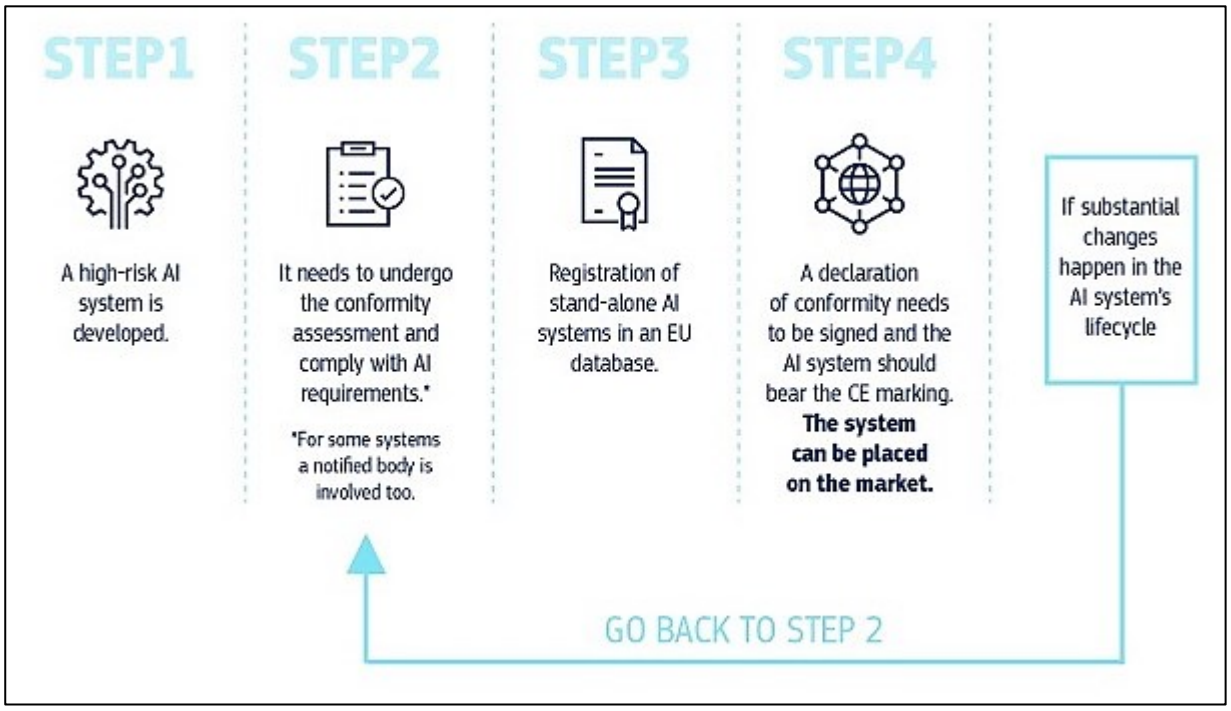
3.5.2 Korkean riskin tekoälyjärjestelmät

EU:n tekoälyasetus määrittelee korkean riskin tekoälyjärjestelmiksi ne, jotka voivat aiheuttaa merkittäviä vaaroja ihmisten terveydelle ja turvallisuudelle tai käyttää tunkeilevia menetelmiä tiedonkeruussa ja profiloinnissa, mikä voi rikkoa perusoikeuksia. Tällaisia järjestelmiä kehittäessä ja käyttäessä on noudatettava tiukempia sääntöjä, jotka asettavat erityisiä vaatimuksia niiden valvonnalle ja sääntelylle. (Kalodanis, Rizomiliotis, Feretzakis, Papapavlou & Anagnostopoulos 2025.)

Asetus tuo mukanaan korkean riskin tekoälyjärjestelmille tiukempaa valvontaa sekä raportointivaatimuksia. Näihin vaatimuksiin organisaation tulee kehittää hallintakehykset, joissa otetaan huomioon sääntely sekä tekniset vaatimukset. Organisaatioiden pitää viimeistään nyt alkaa panostamaan riskienhallintaa sekä laadunvalvontaa. Myös dokumentoinnin tärkeys korostuu asetuksen myötä. (Reese 2025.)

Korkean riskin tekoälyjärjestelmiä saa käyttää EU:ssa vain, jos ne täyttävät tietyt pakolliset vaatimukset. Tarkoituksena on varmistaa, että tällaiset järjestelmät eivät aiheuta vakavaa haittaa EU:n kansalaisten terveyteen, turvallisuuteen tai perusoikeuksiin. Usein tekoälyä sisältävä tuote kuuluu useamman eri EU-lain piiriin esimerkiksi lääkinnällisiä laitteita tai koneita koskeviin sääntöihin. Tällöin tuote voidaan tuoda markkinoille tai ottaa käyttöön vasta, kun se täyttää kaikki siihen sovellettavat lait ja asetukset. (Euroopan parlamentti ja neuvosto 2024.)

Jotta yritysten ei tarvitsisi tehdä turhaa hallinnollista työtä, niille annetaan joustoa siinä, miten ne järjestävät tuotteidensa sääntöjenmukaisuuden käytännössä. Tämä tarkoittaa, että yritykset voivat itse valita parhaan tavan täyttää vaatimukset, kunhan lopputulos vastaa kaikkia sovellettavia EU-lakeja. Korkean riskin tekoälyjärjestelmiksi määritellään vain ne, joilla voi olla vakava vaikutus ihmisten terveyteen, turvallisuuteen tai oikeuksiin. Näin pyritään rajoittamaan sääntelyn vaikutus vain todella merkittäviin järjestelmiin, eikä estämään turhaan kansainvälistä kaupankäyntiä. (Euroopan parlamentti ja neuvosto 2024.)



Kuva 6. Korkean riskin tekoälyjärjestelmien tarjoajille step-by step (Euroopan komissio 2025)

Kuvassa 6 esitellään, kuinka tekoälyjärjestelmä prosessi toimii joko kehitysvaiheessa oleville järjestelmille tai jo markkinoilla oleville järjestelmille.

3.5.3 Ei hyväksyttävä/kestämätön tekoälyjärjestelmä

Tekoälylaki kieltää korkean riskin tekoälyn käytöt, jotka uhkaavat ihmisten oikeuksia tai turvallisuutta, kuten manipulaation, sosiaalisen pisteytyksen, vahingollisen ohjailun ja harhaanjohtamisen tekoälyn avulla, valvontakameroiden aineiston summittaisen keräämisen kasvojentunnistusrekistereihin sekä internetin tai kasvojentunnistuksen valvontakäytön. (Euroopan komissio 2025.)

3.6 Lainvalvontaan liittyvät poikkeukset

Tekoälyasetuksessa on otettu huomioon lainvalvonta tarkoituksessa liittyvä tekoälynkäyttö sekä huomioitu viranomaisten tarpeet. Huomioissa on otettu huomioon lainvalvontaviranomaisten kyky

käyttää tekoälyä ja sen tarpeet. Asetukseen on lisätty erityinen menettely, joka sallii lainvalvontaviranomaisen käyttää tekoälyvälinetä, vaikka ne olisivat vielä keskeneräisiä hyväksynnän kannalta. (Euroopan komissio 2025.)

Reaaliaikaisten biometristen etätunnistusteknologioiden käyttö julkisissa tiloissa on selvennetty erityisesti tilanteisiin, joissa lainvalvontaviranomaisille on välttämätöntä käyttää niitä. Tällöin käyttö rajoittuu poikkeuksellisesti tiettyihin tilanteisiin, kuten vakavien rikosten estämiseen tai rikoksen uhrien löytämiseen. Kompromissiratkaisussa on määritelty tarkempia suojatoimia, jotka varmistavat, että poikkeuksia sovelletaan vain niihin tapauksiin, joissa uhka on todellinen tai ennakoitavissa, kuten terrori-iskujen ehkäiseminen tai vakavien rikosten tekijöiden etsintä. (Euroopan komissio 2025.)

3.7 Esimerkkejä tekoälyjärjestelmistä

Arkielämässä tekoälyjärjestelmiä tulee koko ajan vastaan. Tekoälyä käytetään jo monissa eri muodoissa ja hyödynnytetään jo laajasti esimerkiksi lääketieteessä (Euroopan komissio 2025).

Tekoälysovelluksiin voi törmätä arkielämässä kuten Taulukko 3 esittää:

Taulukko 3. Tekoälysovellukset (Euroopan komissio 2025)

Arkielämässä	**Esimerkki**
Nettiostokset ja mainonta	Kohdennettu mainonta perustuen esimerkiksi heidän aiempiin hakuihinsa tai ostoksiinsa tai muuhun käytökseen verkossa
Hakukoneet	Oppimiseen ja käyttäjille tarjoamiin hakutuloksiin
Digitaaliset avustajat	Virtuaaliavustajat
Konekäännökset	Automaattinen tekstitys tai kääntäminen
Älykkäät kodit, kaupungit ja infrastruktuuri	Kulkuyhteyksien parantaminen
Autot	Turvatoiminnot
Kyberturvallisuus	Datan, mallien tunnistamisen ja toteutettujen iskujen analysointi
Virusturvallisuus	Lämpökamerat yleisillä paikoilla

Disinformaation torjunta	Valeuutisten ja dis informoinnin tunnistaminen
Terveys	Suuren määrän datan analysointi, hätäpuhelut, diagnostiikan parantaminen
Liikenne	Raideliikenteen turvallisuutta, nopeutta ja tehokkuutta vähentämällä rengaskitkaa, maksimoimalla nopeuden ja sallimalla autonomisen ajamisen
Teollisuus	Tehokkuus, robotiikka
Ruoantuotanto	Terveellisempi ja torjunta-aineiden käytön vähentäminen

4 Riskienhallinta

Tekoäly tuo mukanaan laajoja mahdollisuuksia, mutta sen hyödyntäminen edellyttää huolellista riskienhallintaa ja selkeitä vastuunjakoja. Mallien luotettavuuden varmistaminen on ensiarvoisen tärkeää, sillä virheelliset tiedot voivat johtaa vaarallisiin seurauksiin mm. terveydenhuollossa, jossa tekoälyn virheet tai riskit voivat olla merkittävät terveydelle. Monimutkainen ja monitulkintainen lainsäädäntö voi asettaa tarpeettomia esteitä tekoälyn hyödyntämiselle, joten sääntelyn tulisi keskittyä vastuiden selkeyttämiseen ja suojamekanismien määrittämiseen. (Heinäsenaho, Lähesmaa & Äyräs-Blumberg 2023.)

Tekoälyjärjestelmien riskienhallinta tuotekehityksessä eroaa perinteisistä ohjelmistokehityksistä erityisesti siinä, miten tietoturva ja tietosuoja otetaan huomioon. Sen sijaan, että keskityttäisiin vain turvalliseen koodaukseen, tärkeämpää on määritellä tarkasti käyttötilanteet, vaatimukset ja suunnitella turvallinen arkkitehtuuri palvelumuotoilun ja tuotteenhallinnan näkökulmasta. Datan hallinnan ja analyysin osalta periaatteet ovat hyvin samanlaiset kuin perinteisissä IT-järjestelmissä ja keskeisiä asioita ovat esimerkiksi pääsynhallinta ja järjestelmän auditoitavuus. (Heinäsenaho, Lähesmaa & Äyräs-Blumberg 2023.)

Koneoppimismallien tietoturvatestaus on kuitenkin haasteellisempaa, sillä mallien tarkastelu voi poiketa perinteisten järjestelmien testeistä. Koneoppimismalleja on vaikea analysoida staattisesti ja joskus testauksen on jatkuttava jopa sen jälkeen, kun järjestelmä on otettu käyttöön. Dynaaminen testaaminen voi myös olla vaikeaa puutteellisen testidatan ja sen eroavuuden vuoksi todellisista olosuhteista. (Heinäsenaho, Lähesmaa & Äyräs-Blumberg 2023.)

On tärkeää, että tekoälyn erityisriskit tunnistetaan ja niiden hallintaan on toteutettu keinot. Vaikka EU:n tasoisesta säädöksestä on kyse, kannattaa silti myös kansallisella tasolla alkaa varautumaan ja tunnistamaan riskejä. EU tasoisissa organisaatioissa voidaan joskus liikkua liian hitaasti teknologian kehityksen mukana.

Tekoälyn riskienhallinta tuotekehitysprosessissa vaatii kokonaisvaltaista ajattelua, jossa on yhdistettävä tietoturvan, datan käsittelyn ja järjestelmän arkkitehtuurin hallinta. Riskianalyysi ja testausprosessi poikkeavat perinteisestä ohjelmistokehityksestä, mutta oikeanlainen lähestymistapa voi vähentää tekoälyn käyttöön liittyviä riskejä merkittävästi. (Traficom 2021.)

4.1 Asetuksen tuomat lisävaatimukset riskienhallintaan

EU:n tekoälyasetus tuo perinteiseen riskienhallintaan uusia vaatimuksia (katso kuva 7), jotka painottavat ennakointia, jatkuvaa valvontaa ja koko tekoälyjärjestelmän elinkaaren huomioimista. Asetus edellyttää, että riskit arvioidaan jo kehitysvaiheessa ja että tekoälyn toimintaa seurataan järjestelmällisesti sen käyttöönoton jälkeen. Riskienhallinta ei enää koske vain teknisiä uhkia, vaan se ulottuu myös eettisiin, oikeudellisiin ja yhteiskunnallisiin vaikutuksiin, kuten yksityisyydensuojaan ja syrjimättömyyteen. Lisäksi tekoälyjärjestelmät on luokiteltava riskitasojen mukaan, mikä vaatii organisaatioilta kykyä tunnistaa ja perustella sovelluskohtaisten riskien vakavuus. (Piachqaud-Moustakis 2023.)

Kuva 7. Riskienhallinnan uudet vaatimukset

Asetus korostaa myös läpinäkyvyyttä ja dokumentointia, jotka ovat keskeisiä viranomaisvalvonnan ja vastuunjaon kannalta. Toisin kuin perinteinen riskienhallinta, EU:n tekoälyasetuksen mukainen lähestymistapa vaatii monialaista yhteistyötä. Teknologian, lainsäädännön ja etiikan asiantuntijoiden on toimittava yhdessä. Näin tekoälyasetuksen mukainen riskienhallinta muuttuu pelkästä sisäisestä prosessista osaksi sääntelyyn perustuvaa vastuullisuutta ja luotettavuutta. (Piachqaud-Moustakis 2023.)

Walters, al 2023 tutkimuksessa *Complying with the EU AI Act: On which areas should organizations focus when considering compliance with the AIA*? Tarkastellaan, miten organisaatiot voivat valmistautua EU:n tekoälylain vaatimuksiin ja mitkä alueet aiheuttavat eniten haasteita. Kyselyn tulokset osoittavat, että organisaatiot kohtaavat haasteita erityisesti teknisen dokumentaation laatimisessa ja henkilöstön koulutuksessa. Lisäksi mallien ja datan ennakkotarkastuksessa sekä käytettävyysvaatimuksissa on puutteita. Vaikka riskienhallintajärjestelmät ja mallin seuranta toimivat osittain, ne vaativat vielä kehittämistä. (Walters, Dey, Bhaumik & Horsman 2023.)

4.2 Tietoturva

Tekoälyn tietoturva muistuttaa perinteistä IT-järjestelmien tietoturvaa, mutta se saa erityisen painoarvon datan käsittelyn ja analyysin osalta. Koneoppimismallien testaus eroaa perinteisistä menetelmistä erityisesti siksi, että staattinen analyysi ei tarjoa luotettavaa keinoa mallin toiminnan arvioimiseen. Samalla dynaamisen testauksen toteuttaminen voi osoittautua haasteelliseksi, mikäli tarvittavaa testidataa ei ole riittävästi saatavilla. (Traficom 2021.)

Koneoppimismallien jatkuva oppiminen käyttöönoton jälkeen haastaa elinkaaren hallintaa, sillä mallit voivat kehittyä ennakoimattomasti ja omaksua uusia ominaisuuksia. (Traficom 2021).

Perinteinen ohjelmistokehitys keskittyy pääsääntöisesti ohjelmiston turvalliseen toimintaan, mutta koneoppimismalleissa ei voi täysin ennakoida, millaisia haavoittuvuuksia ne voivat kehittää, koska niiden toiminta perustuu datan ja algoritmien kehittymiseen. (Traficom 2021).

Tietoturvan hallinta pitäisi toteuttaa kokonaisvaltaisesti niin, että tuotekehityksen ja IT:n tietoturvatoimet eivät ole toisistaan erillisiä. Tämä on erityisen tärkeää siirryttäessä pilviympäristöihin (cloud-native), joissa myös AI-ratkaisujen integrointi on osattava hallita osaksi laajempaa infrastruktuuria. (Traficom 2021).

4.3 Käyttötapausten ja palvelumuotoilun merkitys

Käyttöönottovaiheeseen ja erityisesti käyttötapauksia mietittäessä voi olla hyödyllistä ottaa huomioon myös mahdolliset negatiiviset käyttötapaukset (esimerkiksi hyökkäykset tai järjestelmän epäonnistuminen). Tämä auttaa minimoimaan systemaattisia riskejä, jotka voivat vaikuttaa tekoälyjärjestelmän toimintaan. (Traficom 2021).

EU:n tekoälyasetus tuo esille vaatimuksia läpinäkyvyyden ja käyttäjien informoinnin suhteen, mikä tulee ottaa huomioon jo palvelumuotoiluvaiheessa. Asetuksen mukaiset riskienhallintakäytännöt

voivat auttaa varmistamaan, että tekoälyjärjestelmät täyttävät eettiset ja lainsäädännölliset vaatimukset. (Traficom 2021).

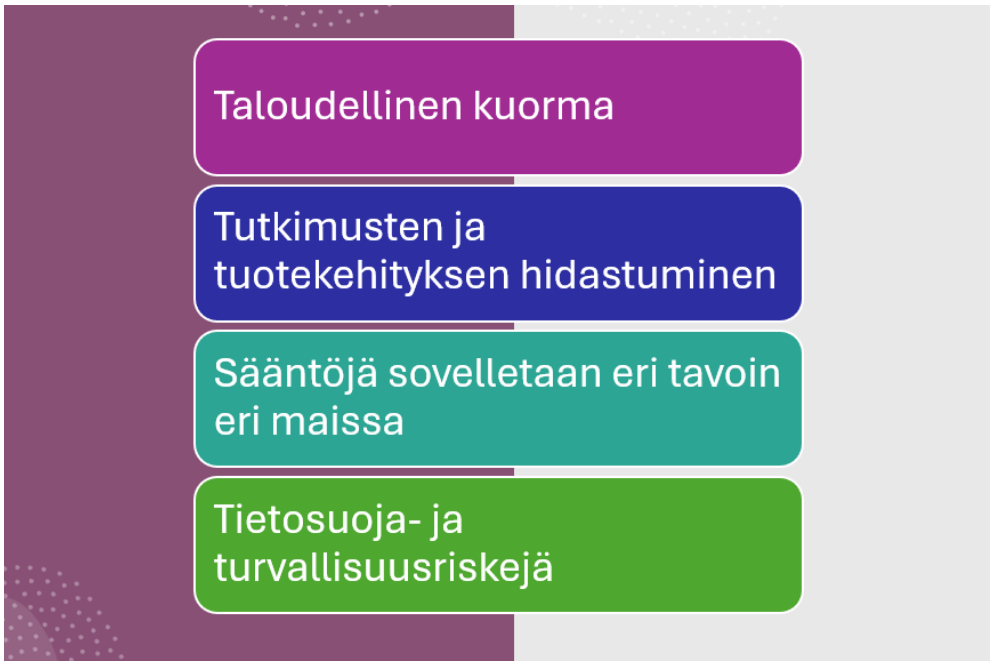
4.4 Arkkitehtuurisuunnittelu ja riskianalyysi

Arkkitehtuuritasolla voidaan suorittaa riskianalyysiä, joka tunnistaa tekoälyjärjestelmän ulkoiset ja sisäiset riskit. Tällöin voidaan suunnitella, miten järjestelmän turvallisuus toteutetaan ja mitkä ovat mahdolliset haavoittuvuudet, jotka voivat tulla esiin järjestelmän käytössä. Hyvä käytäntö voi olla myös luoda prototyyppi ennen tekoälyn integrointia, joka mahdollistaa järjestelmän toiminnan arvioinnin ilman tekoälyn tuomia lisähaasteita. (Traficom 2021).

Poikkeamienhallinta tekoälyjärjestelmissä on tärkeää, sillä mallien väärinkäyttö tai vanheneminen voi johtaa vakaviin turvallisuusongelmiin. Tällöin myös järjestelmän monitorointi on tärkeää, jotta mahdolliset poikkeamat voidaan havaita ajoissa ja reagoida niihin nopeasti. (Traficom 2021).

4.5 Riskit

Yksi merkittävimmistä haasteista, joita EU:n tekoälyasetus tuo mukanaan, liittyy sen monikerroksiseen ja vaativaan sääntelyrakenteeseen. Yritykset joutuvat varautumaan kattaviin hallinnollisiin velvoitteisiin, kuten yksityiskohtaiseen dokumentointiin, algoritmien toiminnan arviointiin ja riskienhallintajärjestelmien rakentamiseen. Tämä voi aiheuttaa huomattavaa taloudellista kuormaa, erityisesti pienille ja keskisuurille toimijoille, joilla ei välttämättä ole riittäviä resursseja vastata samoihin vaatimuksiin kuin suuryrityksillä. Seurauksena voi olla epätasapaino kilpailuedellytyksissä eri kokoisten yritysten välillä. Kuvassa 8 on esitetty sääntelyyn liittyvät riskit. (Kalodanis ym. 2025.)



Kuva 8. Sääntelyn riskit.

Lisäksi asetuksen tiukka sääntelykehys voi vaikuttaa haitallisesti tekoälyyn liittyvään tutkimukseen ja tuotekehitykseen. Organisaatiot saattavat pidättäytyä kokeiluista ja uusista innovatiivisista avauksista, jos niihin liittyy riski sanktioista tai vaatimustenmukaisuuden epäonnistumisesta. Tämä varovaisuus voi hidastaa kehitystä ja vähentää EU:n houkuttelevuutta tekoälyn edelläkävijäalueena verrattuna alueisiin, joissa sääntely on joustavampaa ja tukee ketterämpää innovaatiota. (Kalodanis ym. 2025.)

Asetuksen toimeenpanossa saattaa esiintyä epäjohdonmukaisuutta, koska kunkin EU:n jäsenvaltion on nimettävä omat kansalliset valvontaviranomaisensa. Tämä voi johtaa siihen, että sääntöjä sovelletaan eri tavoin eri maissa. Lisäksi valvontaviranomaisten resurssit ja asiantuntemus voivat olla rajallisia, mikä saattaa heikentää sääntöjen valvonnan ja toimeenpanon tehokkuutta. (Kalodanis ym. 2025.)

Tekoälyjärjestelmien tietojen luovutus sääntelytarkastuksia varten tuo mukanaan tietosuoja- ja turvallisuusriskejä, erityisesti silloin, kun käsitellään arkaluontoisia tai henkilökohtaisia tietoja. Teknologian nopea kehitys voi myös aiheuttaa tilanteen, jossa lainsäädäntö ei pysy mukana uusien innovaatioiden tahdissa, mikä voi johtaa sääntöjen epäselvyyksiin tai siihen, että ne joko rajoittavat liikaa tai eivät ole riittäviä suojellakseen asianmukaisesti. (Kalodanis ym. 2025.)

5 Tutkimuksen tulokset

Tekoälysäädöksen vaatimusten täytäntöönpano vaatii yhteensovittamista sääntelyn, datanhallinnan, compliance-kyvykkyyksien arvioinnin ja kehittämisen, IT-riskienhallinnan, häiriötilanteiden hallinnan sekä raportoinnin osalta. Lisäksi tulee toteuttaa digitaalisen häiriönsietokyvyn testausta, kuten tietoturvatestausta tai penetraatiotestausta (Deloitte 2023).

Jos tekoälyjärjestelmän aiheuttamaa uhkaa tai riskiä ei voida riskienarvioinnin jälkeen hyväksyä, pitää järjestelmän käyttö kieltää (Euroopan parlamentti 2023). Tällaisia riskejä on esitelty taulukossa 4:

Taulukko 4. Tekoälyjärjestelmien kielletyt käyttötapaukset

Kiellettyä	Esimerkki
Yksilöiden tai tiettyjen heikossa asemassa olevien ryhmien käytöksen manipuloiminen	ääniaktivoituvat lelut, jotka kannustavat lapsia vaaralliseen käytökseen
Sosiaalinen pisteytys	ihmisten jakaminen ryhmiin käytöksen, sosioekonomisen aseman tai henkilökohtaisten ominaisuuksien perusteella
Luonnollisten henkilöiden biometrinen tunnistaminen ja luokittelu	Julkisten tilojen kasvojentunniste (massavalvonta)
Reaaliaikainen ja etäisyydeltä tapahtuva biometristen tunnistusjärjestelmien käyttö	Kasvojentunnistaminen
Haitalliset alitajuiset tekniikat	Ihmisten käyttäytymisen manipulointi
Tunteiden tunnistamisjärjestelmät	Työelämässä ja koulutuksessa käytettävät

Joitain poikkeuksia voidaan hyväksyä, jos kyseessä on viranomainen, jolla on erillinen lupa esimerkiksi vakavan rikoksen tutkintaan. Tekoälyjärjestelmät, jotka vaikuttavat turvallisuuteen tai ihmisen perusoikeuksiin luokitellaan suuririskisiksi. Kaikista korkeariskisistä järjestelmistä, jotka tulevat markkinoille, tehdään ensiarvio sekä arviointia jatketaan koko elinkaaren ajan. (Euroopan parlamentti 2023.)

Näitä ovat Euroopan parlamentin mukaan mm.

Tekoälyjärjestelmät, joita käytetään EU:n tuoteturvallisuusdirektiivin alle kuuluvissa tuotteissa	**Mm.** • lelut, • ilmailu • autot • lääkinnälliset laitteet • hissit
Tietyille aloille kuuluvat tekoälyjärjestelmät, jotka tulee rekisteröidä EU-tietokantaan	• kriittisen infrastruktuurin hallinta ja käsittely • yleissivistävä ja ammatillinen koulutus • työllistäminen, henkilöstöhallinto sekä itsenäisen ammatinharjoittamisen mahdollistaminen • olennaisten yksityisten palvelujen ja julkisten palvelujen ja etujen saatavuus ja käyttö • lainvalvonta • muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta • oikeudenhoito ja demokraattiset prosessit

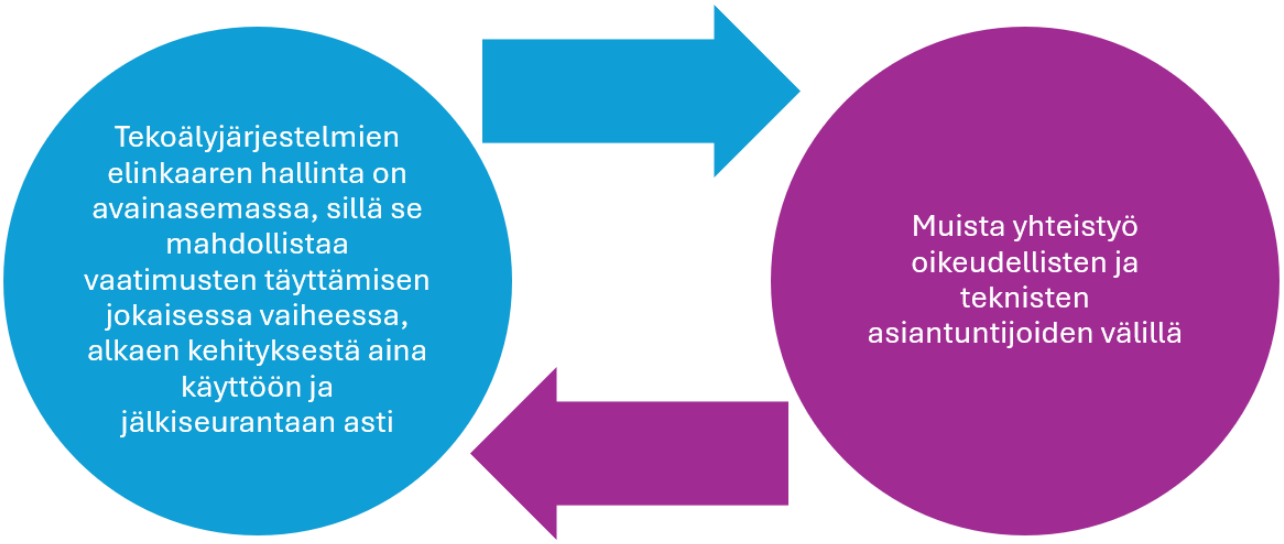
Euroopan komission määritelmän mukaan tekoälyä voi ilmetä kahdessa eri muodossa. Ensimmäinen ilmentymismuoto on ohjelmistoon liittyvä. Tämä voi olla esimerkiksi virtuaalinen avustaja nettisivuilla tai sovelluksessa tai esimerkiksi jonkunlainen hakukone. Toinen on niin sanottu ”ruumiillistettu” muoto. Tällä tarkoitetaan, että tekoäly on robotin muodossa tai vaikka droneina. (Euroopan parlamentti 2020.)

5.1 Asetuksen vaatimukset organisaatioille

Jotta organisaatiot voivat vastata EU AI Act vaatimuksiin, niiden tulee ottaa huomioon seuraavat asiakokonaisuudet (Reese 2025):

- Tekoälysovellusten hallintamallin luominen. Hallintamallikehys täytyy sisältää teknisen asiantuntemuksen.

- Riskienhallinta. Tekoälyjärjestelmien riskiluokitukset sekä riskien kartoittaminen ovat keskeinen osa vaatimusten täyttymistä. Organisaation täytyy varmistua elinkaaren hallinnasta, riskien seurannasta ja valvonnasta.
- Dokumentointi ja valvonta. Organisaatiolla on oltava selkeä prosessi järjestelmien kehittämiseksi siten, että ne huomioivat tietosuojan, avoimuuden ja luottamuksellisen käytön. Näitä täytyy jatkuvasti dokumentoida sekä valvoa. Kuvassa 9 kerrotaan tärkeimmät asiat elinkaarenhallinnan näkökulmasta.
- Henkilöstön kouluttaminen. Tärkeä ja perusteellinen valmistautuminen alkaa henkilöstön kouluttamisella. Jos asetusta ei ole jalkautettu koko organisaation toimintaan, organisaatio ei pysty toimimaan vaatimusten mukaisesti.



Kuva 9. Elinkaarenhallinta.

Elinkaaren hallinta on tärkeää, jotta sääntöjenmukaisuus varmistetaan tekoälyjärjestelmän kaikissa vaiheissa ja voidaan toteuttaa suunnittelussa. Organisaatiot voivat joutua tasapainottelemaan sääntelyn ja innovaation välillä. Vaikka asetukset voivat olla monimutkaisia, niihin voidaan vastata perusteellisella valmistautumisella ja oikealla lähestymistavalla, mikä mahdollistaa innovatiivisen toiminnan jatkamisen organisaation sisällä. (Reese 2025.)

5.2 Organisaatioiden sopeutumistoimenpiteet

Seuraavaksi avataan ja tutkitaan tarkemmin edellä olevien tärkeimpien toimenpiteiden kokonaisuutta.

Inventaario eli nykytilan ymmärtäminen

Ymmärtääkseen EU:n tekoälylain vaikutukset, yritysten tulee ensiksi arvioida, onko niillä tekoälyjärjestelmiä käytössä, kehitteillä tai hankinnassa kolmansilta osapuolilta, ja listata tunnistetut järjestelmät mallivarastoon. Vaikka tekoälyä ei vielä olisi käytössä, on se tulevaisuutta – jokaisella toimialalla näitä ratkaisuja tullaan jossain määrin tarvitsemaan. (Meier 2024.)

Riskienhallinta

Riskienhallinta on keskeinen osa EU:n tekoälyasetusta ja sen velvoitteita. Se luo vankan pohjan organisaation vastuulliselle toimimiselle. Erityisesti riskiluettelon muodostaminen riskeistä on osoittautunut tehokkaaksi monissa organisaatioissa. (Reese 2025.)

Tekoälyjärjestelmien riskiluokitukset edellyttävät järjestelmien tyypin tunnistamista ja niihin liittyvien vaatimusten ymmärtämistä. Esimerkkejä korkean riskin järjestelmistä ovat esimerkiksi kriittiseen infrastruktuuriin, rekrytointiin, työntekijöiden luokitteluun, luottoluokitukseen, vakuutuskorvauksiin ja riskihinnoitteluun liittyvät sovellukset. (Meier 2024.)

Korkean riskin järjestelmät ovat sallittuja, mutta niiden on täytettävä useita vaatimuksia ja niiden on suoritettava vaatimustenmukaisuusarviointi. Tämä arviointi on suoritettava ennen järjestelmien markkinoille saattamista. Nämä järjestelmät on myös rekisteröitävä EU:n perustettavaan tietokantaan. Korkean riskin tekoälyjärjestelmien käyttö edellyttää asianmukaista tekoälyriskinhallintajärjestelmää, kirjausominaisuuksia ja henkilövalvontaa sekä omistajuutta. Matalamman riskin järjestelmiltä edellytetään lähinnä läpinäkyvyyttä – esimerkiksi chatbotin käyttäjälle on ilmoitettava, että vuorovaikutuksessa on tekoäly. (Meier 2024.)

Valmistaudu

Tekoälyjärjestelmien toimittajalla on vastuu varmistaa, että kaikki tekoälyn käytännöt ovat uuden sääntelyn mukaisia. Tämä tarkoittaa riskien arviointia, tietoisuuden lisäämistä, eettistä suunnittelua ja jatkuvaa valvontaa (Meier 2024.)

On tärkeää ymmärtää organisaation nykytilanne, valmistautua asetukseen sekä tiedostaa tekoälyjärjestelmienne käyttötilanteet kuvan 10 mukaisesti. Tämä luo pohjan organisaation ymmärrykselle, mitkä EU:n tekoälyasetuksen osa-alueet koskevat organisaatiotanne ja auttaa ohjaamaan tekoälyjärjestelmiä laadun ja sisäisten standardien osalta. (Reese 2025.)

Kuva 10. Organisaation toimenpiteet

5.3 Tekoälysovellusten hallintamallit

Tekoälyteknologioiden käyttö ja kehitys edellyttävät hyvin määriteltyä hallintamallia, joka tukee vastuullista ja tehokasta sovellusten hyödyntämistä. Tällaisen mallin suunnittelu ja toteutus vaativat erityistä huomiota rooleihin, vastuisiin, riskienhallintaan, eettisiin periaatteisiin ja käytön sääntöihin. Hyvin toimiva hallintamalli perustuu useisiin keskeisiin periaatteisiin, jotka auttavat organisaatioita varmistamaan tekoälyjärjestelmien turvallisuuden ja luotettavuuden. (Karppinen ja Nyqvist 2025.)

Ensimmäinen askel tekoälysovellusten hallintamallin luomisessa on määritellä selkeät roolit ja vastuut. Tärkeimpiä rooleja ovat esimerkiksi tekoälyvastaava, joka valvoo järjestelmän käyttöä ja varmistaa sen eettisyyden, tekoälyarkkitehti, joka suunnittelee ja kehittää tekoälysovelluksia, sekä riskienhallintavastaava, joka arvioi ja hallitsee mahdollisia tekoälyyn liittyviä riskejä. Tämän lisäksi on tärkeää nimetä henkilöitä, jotka vastaavat tekoälyn laadunhallinnasta, varmistavat datan luotettavuuden ja tukevat sovellusten pitkäaikaiskäytön hallintaa. (Karppinen ja Nyqvist 2025.)

Tekoälysovellusten kehittämisessä ja käytössä on keskeistä tunnistaa ja hallita mahdollisia riskejä. Riskienhallinta ei ainoastaan sisällä teknisten riskien arviointia, kuten järjestelmän virheellistä toimintaa, vaan myös laajempia yhteiskunnallisia ja eettisiä riskejä, kuten tekoälyn vaikutuksia yksilöiden oikeuksiin ja tasa-arvoon. Tekoälyn käytön ja kehityksen tulee täyttää kaikki sovellettavat säädökset, kuten GDPR ja kansalliset tekoälysäädökset. Riskienhallintaa tulisi tehdä jatkuvasti arvioiden, sillä tekoälyjärjestelmien toimintaympäristöt ja teknologiat kehittyvät nopeasti. (Karppinen ja Nyqvist 2025.)

Tekoälyjärjestelmiä hyödynnettäessä on tärkeää luokitella sovellukset käyttötapauksen mukaan. Tämä tarkoittaa sitä, että organisaatio määrittelee, minkälaisiin tarkoituksiin tekoälysovelluksia käytetään ja varmistaa, että ne täyttävät kaikki tarvittavat vaatimukset. Esimerkiksi kaupallisten

tuotteiden kehittämisessä käytettävät sovellukset saattavat vaatia erityistä huomiota kaupallisille säädöksille ja käytön eettisyydelle. Tekoälyn soveltuvuuden arviointi auttaa myös tunnistamaan mahdolliset väärinkäytön riskit ja varmistamaan, että sovellukset eivät aiheuta haittaa yksilöiden oikeuksille. (Karppinen ja Nyqvist 2025.)

Tekoälysovellusten tulee olla ymmärrettäviä ja avoimia. Läpinäkyvyys tarkoittaa sitä, että järjestelmän toiminta ja päätöksenteko voidaan selittää käyttäjille ja sidosryhmille. Tämä on erityisen tärkeää silloin, kun tekoälyjärjestelmä tekee päätöksiä, jotka vaikuttavat yksilöiden elämään tai organisaation toimintaan. Tekoälyn päätöksentekoprosessit tulee dokumentoida ja olla valmiita selitettäväksi ulkopuolisille tarkastajille ja käyttäjille. (Karppinen ja Nyqvist 2025.)

Tekoälyteknologioiden jatkuva kehittyminen edellyttää organisaatioilta panostusta koulutukseen ja osaamisen kehittämiseen. Tämä tarkoittaa, että henkilöstön tulee ymmärtää tekoälyjärjestelmien toiminta ja sen vaikutukset omaan työhönsä. Koulutuksen tulee kattaa muun muassa tekoälyn perusteet, käytännön sovellukset ja eettiset kysymykset. Myös johdon koulutus on tärkeää, jotta se voi tukea tekoälyhankkeiden toteutusta ja varmistaa, että organisaation strategiat ovat linjassa tekoälyn kehityksen kanssa. (Karppinen ja Nyqvist 2025.)

Tekoälyn riskienhallinta voidaan toteuttaa NIST:n AI Risk Management Frameworkin (AI RMF) avulla. Tämä kehys tarjoaa organisaatioille rakenteen riskien arvioimiseksi ja hallitsemiseksi. Se sisältää kolme keskeistä vaihetta:

• kartoituksen (Map)

• mittaamisen (Measure)

• ja riskienhallinnan (Manage).

Näiden vaiheiden avulla organisaatiot voivat jatkuvasti seurata tekoälyn sovellusten toimivuutta, arvioida riskejä ja toteuttaa toimenpiteitä mahdollisten ongelmien ratkaisemiseksi. (Karppinen ja Nyqvist 2025.)

Kartoitusvaiheessa organisaatiot voivat tunnistaa tekoälyn käyttöön liittyvät riskit ja arvioida niiden mahdollisia vaikutuksia. Mittaamisvaiheessa on tärkeää asettaa selkeitä mittareita, joilla voidaan seurata sovellusten toimivuutta ja varmistaa, että ne täyttävät asetetut tavoitteet. Riskienhallintavaiheessa puolestaan organisaatiot voivat kehittää toimenpiteitä riskien lieventämiseksi ja varmistaa, että tekoälyn käyttö ei aiheuta haitallisia seurauksia. (Karppinen ja Nyqvist 2025.)

5.4 Yleisen tietosuoja-asetuksen ja tekoälylain yhteensovittaminen

GDPR eli yleinen tietosuoja-asetus tulee huomioida yhdessä tekoälylain kanssa. On todella täkeää varmistaa, että ne tekoälyjärjestelmät, jotka käsittelevät henkilötietoja, noudattavat tietosuojaperiaatteita. Täytyy varmistua henkilötietojen lainmukaisuudesta, oikeudenmukaisuudesta sekä läpinäkyvästi käsitellä tekoälyjärjestelmissä näitä. Viime vuosien aikana tekoälytekniikat ovat kehittyneet räjähdysmäisesti, ja ne ovat mullistaneet eri toimialoja, mikä tuo mukanaan haasteita mm järjestelmien vastuullisuuteen, turvallisuuteen sekä valvontaa. (Data Protection Authority of Belgium 2024.)

Tarvitaan teknisiä ja organisatorisia toimenpiteitä, jotka suojaavat tekoälyjärjestelmien käsittelemiä henkilötietoja. Valvonnalla on tärkeä rooli etenkin korkean riskin tekoälyjärjestelmien kehittämisessä sekä käytössä. GDPR ja AI-Act korostavat henkilötietojen käsittelyn hallintaa koko elinkaaren ajan. Kuitenkin tekoälyjärjestelmät tuovat mukanaan erityisiä riskejä, jotka edellyttävät lisäturvatoimia perinteisten tietosuojakäytäntöjen ohella. Organisaation täytyy tehdä riskitason perusteella teknisiä ja organisatorisa toimenpiteitä. (Data Protection Authority of Belgium 2024.)

AI-Act korostaa ennakoivia toimenpiteitä muun muassa:

- Mahdollisten ongelmien tunnistaminen ja suunnittelu. Mietitään skenaariolähteisesti mikä voisi mennä pieleen tekoälyjärjestelmän kanssa ja kuinka todennäköistä tämä olisi. Tehdään riskiarvioita ja tarkastellaan näitä jatkuvasti. (Data Protection Authority of Belgium 2024.)
- Valvonnan ja testaamisen lisääminen, tehdään suorituskykyyn jatkuvia arviointia mm. Turva-aukkojen ja haavoittuvuuksien tunnistamisessa, puolueellisuuden tarkastamisessa ja päätöksentekoprosessien tarkastamisessa (Data Protection Authority of Belgium 2024).

5.4.1 Päätöksentekoprosessin huomioiminen

Organisaation täytyy varmistua siitä, että tekoälyjärjestelmät eivät tee itsenäisiä päätöksiä kokonaisuudessa vaan ihmisiä on sidottu päätöksentekoprosessiin. Algoritmien puolueettomuus on tärkeää ja kriittisessä päätöksenteossa ei saa luottaa täysin tekoälyyn. (Data Protection Authority of Belgium 2024.)

Esimerkiksi sairaaloissa käytettävät tekoälyjärjestelmät keuhkosyövän diagnosointiin voivat käsitellä arkaluonteista potilastietoa. Tietomurto voisi paljastaa kriittisiä tietoja tai johtaa väärään

diagnoosiin, mikä voi aiheuttaa terveysriskejä ja mainehaittaa. (Data Protection Authority of Belgium 2024.)

GDPR:n mukaiset toimenpiteet, jotka organisaation tulisi tehdä:

- Tietojen salaus ja potilastietojen turvallinen käsittely. Henkilötietojen, erityisesti arkaluonteisten potilastietojen, käsittelyssä ja siirtämisessä tulee käyttää vahvoja salaustekniikoita. (Data Protection Authority of Belgium 2024.)
- Pääsynvalvonnan rajoittaminen. Organisaation on määriteltävä selkeästi, kenellä on oikeus tarkastella, muokata tai poistaa henkilötietoja. (Data Protection Authority of Belgium 2024.)
- Järjestelmien tilannekuva ja järjestelmien testaaminen. Tietojärjestelmien turvallisuutta on seurattava jatkuvasti, ja niihin liittyvät haavoittuvuudet on pyrittävä tunnistamaan ja korjaamaan ennakoivasti. (Data Protection Authority of Belgium 2024.)
- Lokien seuranta. Järjestelmien lokitietoja on valvottava aktiivisesti, jotta mahdollinen poikkeava tai epäilyttävä toiminta voidaan havaita ajoissa. (Data Protection Authority of Belgium 2024.)

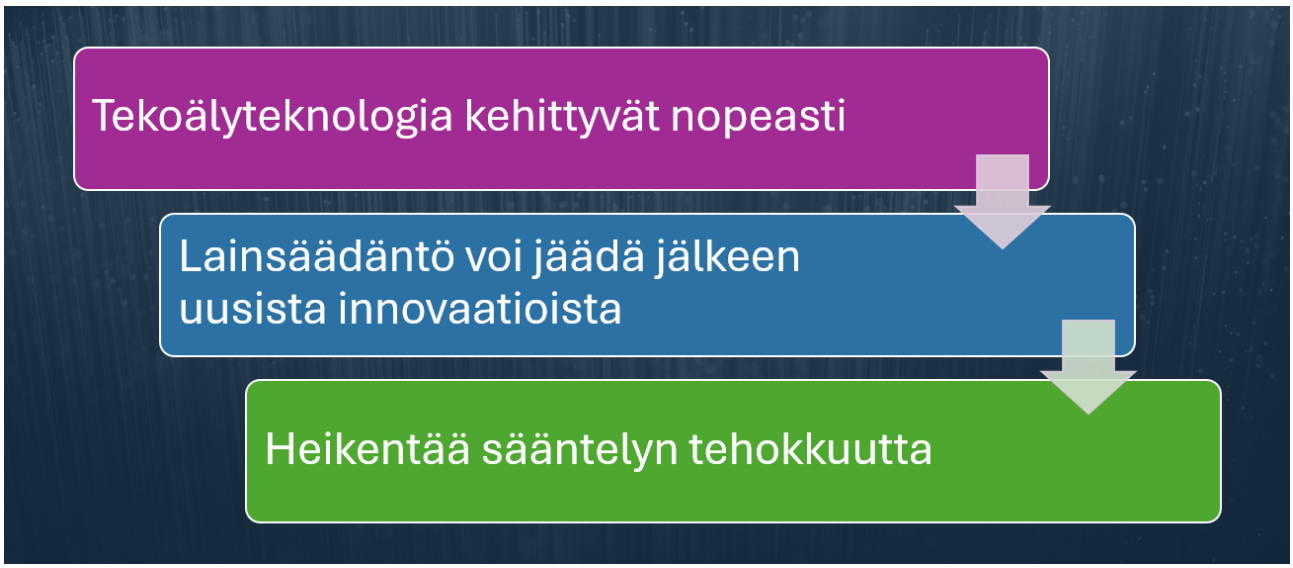
AI-laki vaatii korkeaa turvallisuustasoa korkean riskin tekoälyjärjestelmiltä. Tärkeitä keinoja ovat datan laadun ja eheyden varmistaminen, alkuperän jäljitettävyys sekä inhimillinen tarkistus. Esimerkiksi lääkäreiden arvio epäilyttävistä datapisteistä varmistaa, ettei virheellistä tietoa käytetä koulutusaineistona. Näin voidaan suojata potilasturvallisuus ja varmistaa, että tekoäly toimii luotettavasti ja eettisesti. (Data Protection Authority of Belgium 2024.)

5.5 Haasteita, joita organisaatio voi kohdata

EU AI Act tuo yrityksille haasteita, jotka liittyvät lainsäädännön vaatimuksiin sekä organisaatioiden sisäisiin muutoksiin ja tehtävien uudelleenjärjestelyihin, jotta asetetut vaatimukset voidaan täyttää.

Euroopan unionin kyberturvallisuusviraston mukaan tekoälyn käyttöön liittyvät väärinkäytökset ovat yleistyneet merkittävästi viime aikoina, ja ilmiö herättää yhä enemmän huolta. Vaikka tekoäly tarjoaa merkittäviä mahdollisuuksia eri aloilla, sen rinnalla projektitiimit joutuvat varautumaan uudenlaisiin riskeihin ja uhkakuviin, joita teknologian nopea kehitys tuo mukanaan. Huolenaiheet liittyvät mm. kyberturvallisuuteen ja yksityisyyteen, etenkin kun tekoälyä käytetään luovissa sovelluksissa, joissa käsitellään henkilötietoja. (Kalodanis ym. 2025.)

Suuret yritykset pystyvät sopeutumaan uusiin vaatimuksiin, mutta pienten sekä keskisuurten yritykset voivat kohdata taloudellisia haasteita. Asetus on myös saanut paljon kritiikkiä asiantuntijoilta. Heidän mielestään asetuksella on laaja-alaisia vaikutuksia kansainvälisiin organisaatioihin, jotka toimivat EU:n alueella. (Ratko 2025.)



Kuva 11. EU AI Act ongelmat.

Yksi asetuksen suurimmista haasteista on kehityksen ja sääntelyn yhteensovittaminen. Koska tekoälyteknologia kehittyy nopeasti, lainsäädäntö voi jäädä jälkeen uusista innovaatioista, mikä heikentää sääntelyn tehokkuutta. Tämän vuoksi on tärkeää, että sääntely tasapainottaa kuluttajien ja yhteiskunnan suojelun samalla edistäen innovaatiota ja kilpailukykyä kansainvälisesti. Kuvassa 11 nostetaan esille tekoälyn sääntelyyn liittyvä heikkous. Kun olemme tekemisissä teknologian ja varsinkin sellaisen teknologian kanssa, jossa jo vuodessa tapahtuu suuria muutoksia ja hyppäyksiä teknologisessa mielessä, aiheuttaa tämä suuren ongelman lainsäädännön päivittämisessä. Lainsäädäntö voi jäädä jo ns. ”vanhaksi” sen voimaanastumisen jälkeen. Tämä tarkoittaa sitä, että asetusta olisi tarkasteltava ja päivitettävä vastaamaan teknologisiin muutoksiin. (Kalodanis ym. 2025.)

6 Uusia liiketoimintamahdollisuuksia

Organisaatiot voivat myös hyötyä asetuksista ja avata uusia liiketoimintamahdollisuuksia. Organisaatiot voivat tämän avulla erottautua vastuullisuudella sekä eettisyydellä ja toteuttaa sellaisia ratkaisuja, joita arvostetaan Euroopassa sekä globaalissa markkinassa. Myös kritiikkiä on kohdistunut reaaliaikaisten kasvojentunnistamiseen, jota ei asetuksessa täysin kielletä. (Ratko 2025.)

Asetuksen tarjoama selkeä sääntelykehys lisää läpinäkyvyyttä ja luottamusta tekoälyratkaisuihin, mikä voi parantaa organisaation mainetta ja houkutella uusia asiakkaita erityisesti turvallisuutta ja eettisyyttä painottavilla toimialoilla, kuten terveydenhuollossa ja julkishallinnossa (European Commission 2025). Kilpailuetu voi syntyä siitä, kun yritys noudattaa vaatimuksia jo ennen niiden pakollista soveltamista ja toimii edelläkävijänä alalla. (EY 2024.)

Pk-yrityksille tämä voi tarkoittaa mahdollisuutta kehittää tuotteita sääntelyhiekkalaatikossa, jossa innovaatiota voi testata ilman täyttä sääntelytaakkaa, mutta viranomaisten ohjauksessa (European Parliament, 2024). Asetuksen tuoma harmonisointi EU:n sisämarkkinoilla myös vähentää hallinnollista taakkaa ja helpottaa markkinoille pääsyä, mikä voi edistää yritysten kansainvälistymistä. (KPMG 2024.)

Lisäksi asetuksen vaatimukset esimerkiksi dokumentoinnista, riskienhallinnasta ja ihmisen valvonnasta voivat parantaa sisäisiä prosesseja ja laatua. Tämä voi vaikuttaa positiivisesti asiakastyytyväisyyteen, vähentää virheitä ja lisätä toiminnan tehokkuutta. Samalla tekoälypalveluiden kehittäminen EU AI Actin mukaisesti voi tarjota liiketoimintamahdollisuuksia sertifioinnissa, auditoinnissa ja konsultoinnissa niille organisaatioille, jotka tarjoavat palveluita sääntelyn tueksi. (Deloitte 2023.)

7 Pohdinta

Tekoälyn nopea kehitys ja digitalisaatio ovat tuoneet mukanaan uudenlaisia kyberturvallisuusuhkia, joihin ei nykysäätely tai perinteiset turvatoimet enää riitä. Tekoäly mahdollistaa entistä kehittyneempiä ja tehokkaampia kyberhyökkäyksiä, minkä vuoksi sääntelyn kehittäminen ja turvallisuuden varmistaminen ovat yhä tärkeämpää.

Tutkimuksen päätutkimuskysymys oli: "Miten EU AI Act vaikuttaa organisaatioihin ja mitä riskienhallintaan liittyviä vaatimuksia sen täytäntöönpano edellyttää?" Tutkimuksessa havaittiin, että EU AI Act tuo mukanaan merkittäviä uusia vaatimuksia erityisesti korkean riskin tekoälyjärjestelmiin liittyen, kuten riskinarviointi, läpinäkyvyys, tietoturva sekä tekniset ja dokumentoinnilliset vaatimukset. Korkean riskin tekoälyjärjestelmien käyttö edellyttää asianmukaista tekoälyriskinhallintajärjestelmää, kirjausominaisuuksia ja henkilövalvontaa sekä omistajuutta. Organisaatioiden on vastattava näihin kehittämällä vastuullisen tekoälyn prosesseja ja varmistamalla tekninen ja juridinen asiantuntemus. Tämä tarkoittaa riskien arviointia, tietoisuuden lisäämistä, eettistä suunnittelua ja jatkuvaa valvontaa.

Ensimmäisen alaongelman, eli "Mitä vaatimuksia EU AI Act asettaa tekoälyjärjestelmille?", näkökulmasta sääntelyssä painottuvat erityisesti riskiluokittelu, dokumentointi, käyttäjien koulutus ja valvonnan suunnittelu. Organisaation täytyy varmistua siitä, että tekoälyjärjestelmät eivät tee itsenäisiä päätöksiä kokonaisuudessaan, vaan ihmisiä on sidottu päätöksentekoprosessiin. Lisäksi tekoälyn päätöksentekoprosessit tulee dokumentoida ja olla valmiita selitettäväksi ulkopuolisille tarkastajille ja käyttäjille.

Toisen alaongelman, eli "Miten yritykset voivat sopeutua asetuksen vaatimuksiin?", osalta havaittiin, että organisaatioiden on ymmärrettävä järjestelmiensä nykytila ja luokiteltava ne riskitason mukaan. Tekoälyjärjestelmiä hyödynnettäessä on tärkeää luokitella sovellukset käyttötapauksen mukaan, ja varmistaa, että ne täyttävät kaikki tarvittavat vaatimukset. Ensimmäinen askel tekoälysovellusten hallintamallin luomisessa on määritellä selkeät roolit ja vastuut, jotka tukevat vastuullista ja tehokasta sovellusten hyödyntämistä. Lisäksi tekoälyteknologioiden jatkuva kehittyminen edellyttää organisaatioilta panostusta koulutukseen ja osaamisen kehittämiseen, jotta henkilöstö ymmärtää tekoälyjärjestelmien vaikutukset omaan työhönsä.

Kolmannen alaongelman, eli "Millaisia haasteita organisaatiot kohtaavat sääntelyn käytännön toteutuksessa?", osalta havaittiin, että teknologian nopea kehitys ja sääntelyn monimutkaisuus voivat tuoda erityisesti pienille toimijoille haasteita, kuten hallinnollista kuormaa, dokumentointivelvoitteita ja resurssivaatimuksia. Tärkeitä keinoja vaatimuksiin vastaamisessa ovat datan laadun ja eheyden varmistaminen, alkuperän jäljitettävyys sekä inhimillinen tarkistus erityisesti koulutusdatassa.

Vaikka asetuksen tuomat vaatimukset voivat aluksi aiheuttaa haasteita, samalla ne tarjoavat mahdollisuuksia. Sääntely nähdään myös keinona rakentaa luottamusta, erottautua eettisyydellä ja luoda uusia liiketoimintamalleja.

EU AI Act on yksi maailman ensimmäisistä laajoista tekoälyä säätelevistä kehyksistä. Vaikka tutkimus tarkasteli sääntelyn vaikutuksia yleisellä tasolla, havaittiin, että jatkotutkimukselle olisi tarvetta erityisesti organisaatioiden eri yksiköiden näkökulmasta, kuten IT, lakiosasto, HR tai tietoturvavastuut. Näiden sisäisten vaikutusten tarkempi ymmärrys voisi tukea organisaatioiden valmistautumista ja kehitystä sääntelyn suhteen.

Toinen mahdollinen jatkotutkimuksen kohde liittyy tekoälysääntelyn vaikutusten mittaamiseen. Voiko sääntely esimerkiksi hidastaa tekoälyratkaisujen käyttöönottoa? Lisääkö se kustannuksia? Vai voiko se toisaalta nopeuttaa luottamuksen rakentumista ja lisätä asiakasarvoa? Kehittämällä mittareita, joilla arvioidaan tekoälyasetuksen vaikutuksia organisaation suorituskykyyn, voidaan tukea strategista päätöksentekoa ja perustella investointeja vastuulliseen teknologiaan.

Vaikka EU AI Act on saanut kritiikkiä muun muassa teknologian kehityksen jarruttamisesta, se yrittää kannustaa vastuullisessa kehittämisessä.

8 Ammatillinen kehittyminen osana tutkimustyötä

Tutkimus on tukenut ammatillista kehittymistäni monin tavoin. Opinnoissani olen suorittanut Haaga-Heliassa Tekoälyn perusteet -kurssin sekä Data-analytiikka Pythonilla -kurssin, jotka ovat antaneet hyvän pohjan aiheen ymmärtämiselle. Työharjoittelussa olen käyttänyt tekoälyä päivittäin erilaisten ongelmien ratkaisemisessa ja tiedonhankinnassa. Tutkimus tarjosi mahdollisuuden syventyä tekoälyn sääntelyyn regulaation näkökulmasta, mikä oli itselleni uutta ja mielenkiintoista. Aihe liittyi myös omaan alaani ja nykyisiin työtehtäviini, mikä lisäsi motivaatiota ja sitoutumista projektin edetessä.

Tutkimuksen laatiminen on auttanut kasvattamaan omaa ammattitaitoa sekä olen reflektoinut omaa oppimistani prosessin aikana. Koen, että olen saanut kurssien ja tutkimuksen aikana kasvatettua omaa asiantuntijuutta sekä syventää ymmärrystäni tekoälystä ja sen tuomista mahdollisuuksista sekä haasteista. Olen saanut mahdollisuuden syventyä tiettyyn aiheeseen, joka liittyy vahvasti myös omaan ammattiini sekä työtehtäviini. Valitsin aiheen, joka on ajankohtainen ja kiinnostava itselleni, joka antoi motivaatioita kirjoittamiseen. Syventyminen aiheeseen ja sen tutkiminen auttoivat minua ymmärtämään uudella tavalla paitsi teoriaa, myös käytännön haasteita, joita voi esiintyä työelämässä.

Osana prosessia opin myös analysoimaan ja käsittelemään suuria tietomääriä, mikä on hyödyllistä monilla työelämän osa-alueilla. Tutkimus vaatii myös kriittistä ajattelua ja minun täytyi arvioida jatkuvasti mitkä lähteet sopivat oman tutkimukseeni ja mitkä ovat tavoitteeni kirjoituksessa. Tämä kehitti kykyäni arvioida tietoa ja tehdä perusteltuja johtopäätöksiä.

Tutkimuksessa kehitin myös omia ajanhallintaitojani. Kirjoitusprosessi oli pitkä ja vaati aikaansa aineiston keruun, analyysin ja kirjoittamiseen. Tutkimuksen kirjoittaminen vaatii tehokasta aikatauluttamista ja kykyä työskennellä itsenäisesti ja määrätietoisesti.

Tekstin kirjoittaminen kehitti kirjoitustaitojani ja tieteellistä viestintää. Opin jäsentelemään ajatukseni selkeästi ja loogisesti. Lisäksi opin, miten tärkeää on osata kirjoittaa tiiviisti ja esittää väitteet perustellusti. Prosessi oli kannattava ja opin arvioimaan omaa kehittymistäni. Pystyin tarkastelemaan kuinka pitkälle olin kehittynyt alustavasta suunnitelmasta itse valmiiseen tutkimukseen. Huomasin myös, mitkä osa-alueet kaipaavat kehittämistä. Reflektointi auttoi ymmärtämään mitkä ovat vahvuuteni ja kehitysalueeni, joita voin jatkossa kehittää ja käyttää hyödyksi. Ammattimaiseen kehittymiseen kuuluu kyky oppia virheistä ja kehittää itseään jatkuvasti. Tutkimus oli loistava harjoitus tälle itsearvioinnille ja se auttoi minua valmistautumaan työelämän vaatimuksiin, joissa jatkuva oppiminen ja itsensä kehittäminen ovat keskeisiä tekijöitä.

Tutkimus ei ollut vain suoritus, joka piti tehdä valmistuakseni vaan se antoi myös tärkeän ensiaskeleen ammatilliseen kehittymiseeni. Työ auttoi minua syventämään asiantuntijuuttani, kehittämään tutkimus- ja analyysitaitojani, parantamaan ajanhallintaa ja projektinhallintataitoja. Tutkimus oli siis enemmän kuin vain lopputyö, se oli prosessi, josta sain ensiaskeleet uuden työelämän aloittamiseen.

Lähteet

Asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäädös). Euroopan parlamentti ja neuvosto. EUVL L 168, 13.6.2024. Luettavissa: https://eur-lex.europa.eu/eli/reg/2024/1689/oj. Luettu: 15.4.2025.

Data Protection Authority of Belgium. 2024. Artificial Intelligence Systems and the GDPR – a Data Protection Perspective. Luettavissa: https://www.autoriteprotectiondonnees.be/publications/artificial-intelligence-systems-and-the-gdpr---a-data-protection-perspective.pdf. Luettu: 8.2.2025.

Deloitte. 2023. European Union Artificial Intelligence Act. Luettavissa: https://www2.deloitte.com/nl/en/pages/risk/articles/european-union-artificial-intelligence-act.html. Luettu: 26.1.2025.

Deloitte. 2023. Tekoälysäädös pähkinänkuoressa – vaikutukset finanssialalle. Luettavissa: https://www.deloitte.com/fi/fi/Industries/financial-services/perspectives/artificial-intelligence-act-tekoalysaados-finanssiala.html. Luettu: 26.1.2025.

Enisa. 2020. AI Cybersecurity Challenges. Luettavissa: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Artificial%20Intelligence%20Cybersecurity%20Challenges.pdf. Luettu: 1.5.2025.

Euroopan komissio. 2024. EU:n tekoälysäädös tulee voimaan. Luettavissa: https://digital-strategy.ec.europa.eu/fi/news/european-artificial-intelligence-act-comes-force. Luettu: 25.1.2025.

Euroopan komissio. 2025. AI Act. Luettavissa: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai. Luettu: 15.4.2025.

Euroopan komissio. 2025. General-Purpose AI Code of Practice. Luettavissa: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice. Luettu: 19.4.2025.

Euroopan parlamentti. 2020. Mitä tekoäly on ja mihin sitä käytetään? Luettavissa: https://www.europarl.europa.eu/topics/fi/article/20200827STO85804/mita-tekoaly-on-ja-mihin-sita-kaytetaan. Luettu: 26.1.2025.

Euroopan parlamentti. 2023. EU:n tekoälysäädös on ensimmäinen laatuaan. Luettavissa: https://www.europarl.europa.eu/topics/fi/article/20230601STO93804/eu-n-tekoalysaados-on-ensimmainen-laatuaan. Luettu: 25.1.2025.

Euroopan parlamentti. 2024. EU AI Act: first regulation on artificial intelligence. Luettavissa: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence. Luettu: 25.1.2025.

Euroopan unioni. 2024. Yleinen tietosuoja-asetus. Luettavissa: https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm. Luettu: 10.2.2024.

EY. 2024. The EU AI Act: What it means for your business. Luettavissa: https://www.ey.com/en_ch/insights/forensic-integrity-services/the-eu-ai-act-what-it-means-for-your-business. Luettu: 27.1.2025.

Heinäsenaho, M., Lähesmaa, J. & Äyräs-Blumberg, O. 2023. Tekoäly mullistaa terveydenhuoltoa – riskit voidaan torjua suunnittelulla ja yhteistyöllä. Luettavissa: https://stm.fi/-/tekoaly-mullistaa-terveydenhuoltoa-riskit-voidaan-torjua-suunnittelulla-ja-yhteistyolla. Luettu: 5.3.2025.

ISO. 2018. ISO 31000:2018. Risk management Guidelines. Luettavissa: https://www.iso.org/standard/65694.html. Luettu: 15.2.2024.

Kalodanis, K., Rizomiliotis, P., Feretzakis, G., Papapavlou, C. & Anagnostopoulos, D. 2025. High-Risk AI Systems—Lie Detection Application. Future Internet. Luettavissa: https://www.proquest.com/docview/3159470915. Luettu: 19.4.2025.

Karppinen, J. & Nyqvist, A. 2025. Tekoälysovellusten sääntelystä ja tekoälyratkaisuiden riskienhallinnasta. Luettavissa: https://teknologiateollisuus.fi/digipooli/tekoalysovellusten-saantelysta-ja-tekoalyratkaisuiden-riskienhallinnasta/. Luettu: 15.3.2025.

KPMG. 2024. How the EU AI Act affects US-based companies. Luettavissa: https://kpmg.com/us/en/articles/2024/how-eu-ai-act-affects-us-based-companies.html. Luettu: 1.5.2025.

Kusche, I. 2024. Possible harms of artificial intelligence and the EU AI act: fundamental rights and risk. University of Bamberg, Germany. Luettavissa: https://www.tandfonline.com/doi/pdf/10.1080/13669877.2024.2350720. Luettu: 1.5.2025.

Microsoft. 2024. Tutkimus: Suomi Pohjoismaiden kärjessä tekoälyn käyttöönotossa. Luettavissa: https://news.microsoft.com/fi-fi/2024/04/16/tutkimus-suomi-pohjoismaiden-karjessa-tekoalyn-kayttoonotossa/. Luettu: 8.2.2025.

Oikeusministeriö. 2022. Perus- ja ihmisoikeusvaikutusten arviointi lainvalmistelussa. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/164464/OM_2022_15_SO.pdf. Luettu: 22.4.2025.

Parviainen, I. 2024. Generatiivinen tekoäly mullistaa maailmaa. Sisäministeriö. Luettavissa: https://valtioneuvosto.fi/-/1410869/generatiivinen-tekoaly-mullistaa-maailmaa. Luettu: 9.2.2024.

Piachqaud-Moustakis, B. 2023. The EU AI Act. Luettavissa käyttäjätunnuksilla: https://haaga-helia.finna.fi/ExternalAuth/EzproxyLogin?url=ezp.2aHR0cHM6Ly9yZXNlYXJjaC5lYnNjby5jb20vYy9pYnB4YTcvdmlld2VyL3BkZi9qcnJlbnI2cWpyP3JvdXRlPWRldGFpbHM-. Luettu: 23.4.2025.

Ratko, I. 2025. Transformation and Economic Aspects of Software Engineering through the Implementation of the EU AI Act. Luettavissa: https://casopis.pravni-fakultet.edu.rs/index.php/ltp/article/view/875/749. Luettu: 23.4.2025.

Reese, H. 2025. EU AI Act: European AI Regulation and its Implementation. Luettavissa: https://www.pwc.de/en/risk-regulatory/responsible-ai/european-ai-regulation-and-its-implementation.html#questionnaire. Luettu: 15.4.2025.

Traficom. 2021. Tekoälyn soveltamisen kyberturvallisuus ja riskienhallinta. Luettavissa: https://www.traficom.fi/sites/default/files/media/publication/Teko%C3%A4lyn%20soveltamisen%20kyberturvallisuus%20ja%20riskienhallinta.pdf. Luettu: 3.3.2024.

Työ- ja elinkeinoministeriö. 2025. EU:n tekoälyasetus: tekoälykäytäntöjen kiellot astuvat voimaan 2.2.2025. Luettavissa: https://valtioneuvosto.fi/-/1410877/eu-n-tekoalyasetus-tekoalykaytantojen-kiellot-astuvat-voimaan-2.2.2025. Luettu: 9.8.2025.

Valtioneuvosto. 2024. Suomen kyberturvallisuusstrategia 2024–2035. Luettavissa: https://julkaisut.valtioneuvosto.fi/handle/10024/165860. Luettu: 3.3.2024.

Valtioneuvosto 2025. Yhteiskunnan turvallisuusstrategia 2025. Turvallisuuskomitea. Luettavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/166024/VN_2025_1.pdf?sequence=4&isAllowed=y Luettu: 9.2.2024.

Walters, J., Dey, D., Bhaumik, D. & Horsman, S.2023. Complying with the EU AI Act: On which areas should organizations focus when considering compliance with the AIA? Amsterdam University of Applied Sciences. Luettavissa: https://arxiv.org/abs/2307.10458. Luettu: 1.5.2025.

Työssä on käytetty tekoälyä lauseenrakenteiden tarkastamiseen ja korjaukseen.