Tampereen ammattikorkeakoulu

EU:n tekoälysäädöksen vaikutus teknologiateollisuuteen

Nea Luusua

OPINNÄYTETYÖ
Huhtikuu 2025

Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Automaatio

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Sähkö- ja automaatiotekniikan tutkinto-ohjelma
Automaatiotekniikka

LUUSUA, NEA:
EU:n tekoälysäädöksen vaikutus teknologiateollisuuteen

Opinnäytetyö 35 sivua
Huhtikuu 2025

Opinnäytetyössä perehdytään EU:n tekoälysäädöksen (EU 2024/1689) sisältöön kokonaisuudessaan ja selvitetään mitä vaikutuksia se tuo tekoälyjärjestelmien hyödyntämiseen teknologiateollisuuden eri yrityksissä. Opinnäytetyössä tarkastellaan mitä velvoitteita säädös asettaa ja kuinka niihin voidaan valmistautua.

Työ koostuu tekoälysäädöksen sisällöstä yleisesti, tekoälyjärjestelmien riskiluokittelusta, säädöksen tuomista mahdollisuuksista ja haasteista. Näitä kaikkia aiheita peilataan teknologiateollisuuden alojen yrityksien toimintaan. Työssä käsitellään myös tekoälyn standardoinnin vaikutusta lainsäädäntöön, tekoälyn vinoumia sekä eettisyyteen liittyviä aiheita.

Työ toteutettiin kirjallisuustutkimuksena, jossa lähdeaineistona käytettiin pääosin säädöstekstin lisäksi Euroopan komission tuottamaa sekä teknologiateollisuuden alojen tai yhdistysten materiaalia.

Opinnäytetyö toteutti sille asetetut tavoitteet ja tuloksena saatiin yhteenveto tekoälysäädöksen sisällöstä ja sen oleellisimmista vaikutuksista teknologiateollisuuden alojen yrityksiin. Lopullinen vaikutus tekoälysääntelyn vaikutuksista voidaan nähdä vasta tulevaisuudessa, mutta tutkimuksen perusteella on selvää, miksi sääntely on tärkeää ihmisoikeuksien sekä turvallisemman tulevaisuuden takaamiseksi.

Asiasanat: tekoälysäädös, tekoäly, teknologiateollisuus

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Electrical and Automation Engineering
Automation Engineering

LUUSUA, NEA:
The Impact of the EU AI Act on the Technology Industry

Bachelor's thesis 35 pages
April 2025

This thesis explored the content of the EU Artificial Intelligence Regulation (EU 2024/1689) in its entirety and examined the implications it brings for the use of AI systems in various companies within the technology industry. The thesis analysed the obligations introduced by the regulations and explores how companies can prepare for them.

The thesis covered the overall content of the AI Act, the risk classification of AI systems as well as the opportunities and challenges brought by the regulation. These topics were examined through the lens of companies operating in various sectors of the technology industry. The thesis also discussed the role of AI standardization in legislation, algorithmic bias and ethical considerations related to artificial intelligence.

The thesis was conducted as a literature review, using primarily the regulation text itself, materials produced by the European Commission and publications from organizations and associations within the technology industry.

The thesis fulfilled its goals and resulted in a summary of the AI Act’s content and its most significant impacts on the technology industry companies. While the full impact of AI regulation will only be observable in the long term, the findings of this study underscore the critical role of regulatory frameworks in upholding human rights and promoting a safer and more secure future.

Key words: artificial intelligence act, artificial intelligence, technology industry

SISÄLLYS

1 JOHDANTO 6
2 TEKOÄLYSÄÄDÖS 7
2.1 Tekoälysäädöksen rikkominen ja sakot 8
2.2 Keskeiset toimijat 8
2.3 Lain valvontamenetelmät 11
2.4 Tekoälyjärjestelmän ja yleiskäyttöisen tekoälymallin määritelmät 11
2.5 Vinoumat 12
3 TEKOÄLYJÄRJESTELMIEN RISKILUOKITTELU 14
3.1 Kestämätön riski – kielletyt käyttötapaukset 14
3.1.1 Esimerkkejä kielletyistä järjestelmistä 15
3.2 Suuri riski 16
3.2.1 Poikkeukset muissa käyttötapauksissa 17
3.3 Suuririskisten järjestelmien vaatimukset 18
3.3.1 Riskinhallintajärjestelmä 18
3.3.2 Data ja datanhallinta 18
3.3.3 Tekninen dokumentaatio 18
3.3.4 Tietojen säilyttäminen 20
3.3.5 Avoimuus ja tietojen antaminen käyttöönottajille 20
3.3.6 Ihmisen suorittama valvonta 20
3.3.7 Tarkkuus, vakaus ja kyberturvallisuus 21
3.4 Rajoittunut riski 21
3.5 Minimaalinen riski 21
4 TEKOÄLYN STANDARDOINTI 23
5 SÄÄNTELYN TUOMAT HAASTEET JA MAHDOLLISUUDET 26
6 VAIKUTUKSET TEKNOLOGIATEOLLISUUDEN ALAN YRITYKSIIN 28
6.1 Turvakomponentit 28
6.2 Yleiskäyttöiset tekoälymallit 29
6.3 HR-järjestelmät 29
6.4 Tekoälyä kehittävät yritykset 30
6.5 Valmistautuminen ja koulutus 30
6.6 Tekoälyn sääntelyn testiympäristöt 31
7 POHDINTA 32
LÄHTEET 33

LYHENTEET JA TERMIT

EU	Euroopan unioni
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
SFS	Suomen Standardisoimisliitto

1 JOHDANTO

Tekoäly kehittyy nopeasti sen sovellusalueet laajenevat eri toimialoilla. Tekoälyä hyödyntävien järjestelmien käyttö tuo mukanaan useita hyötyjä, se helpottaa ja tehostaa monia prosesseja. Nopean kehityksen ja positiivisten vaikutusten lisäksi tuo se mukanaan kuitenkin kysymyksiä Euroopan unionin arvojen näkökulmasta. EU pyrkii tekoälysäädöksellä (EU) 2024/1689 turvaamaan ihmisen perusoikeuksia ja olemaan turvallisen tekoälykehityksen kärki. Tavoitteena on saada Euroopasta samalla teknologisesti edistyksellinen, mutta myös ihmisoikeuksia kunnioittava ja turvallinen toimintaympäristö.

Tekoälysäädös on maailmanlaajuisesti ensimmäinen tekoälyä koskeva ja sen riskeihin puuttuva laaja-alainen oikeudellinen kehys. Säädöksellä halutaan turvata suoja ihmisten terveydelle, turvallisuudelle ja perusoikeuksille tekoälyjärjestelmien käytöstä aiheutuvilta vaaroilta sekä varmistaa eurooppalaisten luottamusta tekoälyyn.

Säädös koskee niin EU:n alueen toimijoita, kuin EU:n markkinoille pyrkiviä toimijoita, joten myös EU:n ulkopuolelta tulevat tekoälyjärjestelmien toimijat ovat lain piirissä. (Euroopan unioni 2024)

Tämän opinnäytetyön tavoitteena on analysoida tekoälysäädöksen keskeistä sisältöä sekä sen vaikutuksia teknologiateollisuuden alojen yrityksiin. Työssä tarkastellaan millaisia velvoitteita säädös asettaa tekoälyjärjestelmien kehittäjille ja käyttäjille sekä miten sääntely muokkaa tekoälyn tulevaisuutta Euroopan unionin jäsenmaissa.

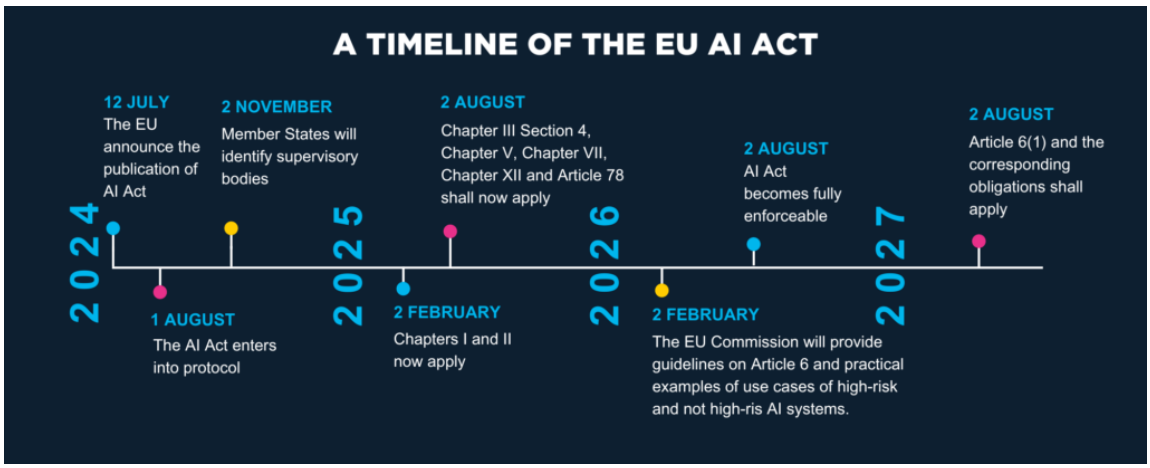
2 TEKOÄLYSÄÄDÖS

EU:n tekoälysäädöksen tavoite on taata, ettei markkinoille tuodut tai käyttöön otettavat tekoälyjärjestelmät aiheuta uhkaa ihmisten turvallisuudelle, terveydelle tai perusoikeuksille. EU haluaa myös yhdenmukaistetulla tekoälylainsäädännöllä parantaa sisämarkkinoiden toimintaa ja tukea innovointia. Säädös määrittää yhteiset käytännöt tekoälyjärjestelmien tarjoamiselle, käyttöönotolle ja käytölle EU:n alueella. Sääntely kohdistuu etenkin haitallisiin käyttötapauksiin. Vaarallisimmat kestämättömän riskin käyttötapaukset kielletään ja suuririskisille tekoälyjärjestelmille asetetaan tiukemmat vaatimukset. (Työ- ja elinkeinoministeriö 2025)

Säädös perustuu riskilähtöiseen lähestymistapaan ja riskit jaetaan neljään eri tasoon: kestämätön, suuri, rajoittunut ja minimaalinen riski. Näille eri riskitasoille vahvistetaan erilliset säännöt, mitä suurempi riski sitä tiukemmat säännöt säädös asettaa. Lainsäädännöllä puututaan tekoälyn luomiin riskeihin, kuten vinoumiin ja syrjintään sekä edistetään innovointia ja kannustetaan tekoälyn käyttöönottoon. (Euroopan unionin neuvosto 2024)

Säädös on yksi osa suurempaa EU:n toimenpidekokonaisuutta, jolla tuetaan tekoälyn kehittämistä. Kokonaisuuteen sisältyy lisäksi tekoälyn innovointipaketti, tekoälytehtaiden käynnistäminen ja koordinoitu tekoälysuunnitelma.
Tekoälytehtaat ovat systeemejä, joiden tavoitteena on edistää yhteistyötä Euroopan alueella ja yhdistää eri alojen toimijoita.

Tekoälysäädös astui voimaan 1. elokuuta 2024, ja sen soveltaminen etenee vaiheittain. 1. helmikuuta 2025 alkaen, säädöstä on alettu soveltamaan kiellettyjen, korkean riskin tekoälyjärjestelmien osalta. Täysimääräisesti säädöstä sovelletaan 2. elokuuta 2026 alkaen. (kuva 1)



KUVA 1. Säädöksen soveltamisaikataulu (Fscom, 2024)

2.1 Tekoälysäädöksen rikkominen ja sakot

Säädöksessä kiellettyjä käytäntöjä rikkoessa voi komissio määrätä sakot, joilla varmistetaan velvoitteiden täyttäminen. Kiellettyjen käytäntöjen rikkomisesta seuraa sakot, jotka ovat määrältään enintään 35 miljoonaa euroa tai 7 % liikevaihdosta. Yleiskäyttöisten tekoälymallien osalta sekä asetuksen muiden vaatimusten rikkominen johtaa sakkoihin, jotka ovat enintään 15 miljoonaa euroa tai 3 % liikevaihdosta. Mikäli yritys toimittaa virheellisiä tietoja viranomaisille, seuraa siitä sakko, joka on enintään 7,5 miljoonaa euroa tai 1,5 % liikevaihdosta. (Teknologiateollisuus ry 2025)

2.2 Keskeiset toimijat

Keskeisiä toimijoita, joihin säädös vaikuttaa koko tekoälyjärjestelmän elinkaaren ajan ovat käyttöönottaja, tarjoaja, jakelija, maahantuoja ja valtuutettu edustaja. Kuvassa 2 selitettynä, mitä nämä tarkoittavat. (EU 2024/1689)

KUVA 2. Keskeiset toimijat

Näillä keskeisillä toimijoilla on velvollisuus noudattaa heille asetettuja vaatimuksia.

Tarjoajan tulee tehdä järjestelmälle vaatimustenmukaisuuden arviointi, jolla osoitetaan sen täyttävän luotettavaan tekoälyyn kohdistuvat vaatimukset. Tarjoajalla tulee olla käytössä kaikki tieto, jonka avulla on varmistettavissa tekoälyjärjestelmän olevan turvallinen ja säädöksen vaatimusten mukainen.
Tarjoajien vastuulla on myös se, että ihmisen kanssa vuorovaikutuksessa olevat tekoälyjärjestelmät ovat selkeästi tunnistettavissa tekoälyä käyttäviksi järjestelmiksi. Vastuulla on myös pitää huolta, että tekoälyllä luodut tuotokset ovat merkitty koneluettavalla merkinnällä ja näin tunnistettavissa tekoälyn luomiksi. (Euroopan komissio 2024)

Käyttöönottajan tulee käyttää ja valvoa järjestelmää käyttöohjeiden mukaisesti, annettava järjestelmän valvonta sellaisille henkilöille, joilla on tähän riittävä osaaminen, varmistaa syöttötietojen olevan merkityksellisiä ja tarpeeksi edustavia ottaen huomioon järjestelmän käyttötarkoituksen. Käyttöönottajan on informoitava valvontaviranomaisia sekä järjestelmän tarjoajaa, mikäli havaitsee riskin sekä säilyttää järjestelmän automaattisesti luoma data vähintään kuuden kuukauden ajan. Työnantajan roolissa käyttöönottajan on kerrottava henkilöstölle uuden järjestelmän käyttöönotosta sekä informoida luonnollista henkilöä, joihin järjestelmän päätöksenteko tai siihen avustavan järjestelmän kohdistuu. (Teknologiateollisuus 2024)

Jakelijan vastuu on ennen järjestelmän markkinoille saattamista tarkastaa, että se sisältää vaaditun CE-merkinnän ja järjestelmän mukana on jäljennös EU-vaatimustenmukaisuus vaatimuksesta eli asiakirja, jolla vakuutetaan järjestelmän olevan EU:n vaatimustenmukainen. (EU 2024/1689)

Maahantuojan velvollisuus on varmistaa ennen järjestelmän saattamista markkinoille, että järjestelmän tarjoaja on suorittanut asianmukaisen vaatimustenmukaisuuden arvioinnin, laatinut asetuksen vaatiman teknisen dokumentaation ja että järjestelmällä on CE-merkintä, EU-vaatimustenmukaisuusvakuutus ja käyttöohjeet. Lisäksi maahantuojan tulee varmistaa, että tarjoaja on nimittänyt valtuutetun edustajan. Mikäli maahantuoja katsoo riittävin syin, ettei järjestelmä ole asetuksen mukainen, se ei saa saattaa järjestelmää markkinoille ennen sen toteamista vaatimusten mukaiseksi. Jos järjestelmä aiheuttaa ihmisen perusoikeuksiin, turvallisuuteen tai terveyteen kohdistuva riskin, tulee maahantuojan ilmoittaa asiasta tarjoajalle, valtuutetulle edustajalle sekä markkinavalvontaviranomaisille.

Valtuutetun edustajan rooli on varmistaa, että EU:n ulkopuolisten tarjoajien järjestelmät täyttävät säädöksen vaatimukset, kun ne tuodaan markkinoille tai otetaan käyttöön EU:n sisällä. Valtuutettu edustaja toimii myös tarjoajien unioniin sijoittautuneena yhteyshenkilönä. (EU 2024/1689)

2.3 Lain valvontamenetelmät

Jokainen EU-valtio nimeää kansallisen valvontaviranomaisen, jonka tehtävä on vastata asetuksen täytäntöönpano omassa maassaan. Tähän tehtävään nimetty viranomainen valvoo tekoälyjärjestelmien käyttöä, tutkii mikäli tulee rikkomuksia sekä ohjaa yrityksiä säädöksen noudattamisessa. Työ- ja elinkeinoministeriö (TEM) on perustanut työryhmän, joka valmistelee lain toimeenpanoa Suomessa. (Työ- ja elinkeinoministeriö 2025)

EU on perustanut myös tekoälyneuvoston, sen tehtävänä on neuvoa ja avustaa EU:n jäsenvaltioita sekä Euroopan komissiota soveltamaan asetusta johdonmukaisesti ja tehokkaasti. Tekoälyneuvostoon kuuluu yksi edustaja kutakin jäsenvaltiota kohden. (Työ- ja elinkeinoministeriö 2025)

Näiden lisäksi tekoälyasetuksessa mainitaan perusoikeuksia suojelevat viranomaiset. Näitä ovat Suomessa:

- Tietosuojavaltuutettu
- Yhdenvertaisuusvaltuutettu
- Tasa-arvovaltuutettu
- Yhdenvertaisuus- ja tasa-arvolautakunta
- Valtioneuvoston oikeuskansleri
- Eduskunnan oikeusasiamies
- Työsuojeluviranomainen (aluehallintovirastot)
- Kuluttaja-asiamies

Edellä mainittujen viranomaisten tulee tarvittaessa pyytää markkinavalvontaviranomaista testaamaan tekoälyjärjestelmä teknisin keinoin, selvittääkseen onko perusoikeuksia rikottu. (Työ- ja elinkeinoministeriö 2025)

2.4 Tekoälyjärjestelmän ja yleiskäyttöisen tekoälymallin määritelmät

Tekoälyjärjestelmä on vaihtelevilla autonomian tasoilla toimivaksi suunniteltu konepohjainen järjestelmä. Se tulkitsee vastaanottamaansa syötettä ja tuottaa sen perusteella erilaisia tuotoksia kuten ennusteita, suosituksia ja päätöksiä, joilla voi olla vaikutuksia fyysisiin tai digitaalisiin ympäristöihin. (EU 1689/2024)

Yleiskäyttöinen tekoälymalli on yleisluonteinen suurella määrällä dataa koulutettu malli, joka on suunniteltu suorittamaan laaja-alaisesti erilaisia tehtäviä. Yleiskäyttöiset mallit esimerkiksi suuret kielimallit ovat sovellettavissa laaja-alaisesti erilaisiin järjestelmiin. (Euroopan komissio 2025)

Yleiskäyttöisille tekoälymalleille on säädöksessä kuvattu kaksi riskiluokkaa.

1. Kaikki yleiskäyttöiset tekoälymallit

2. Yleiskäyttöiset tekoälymallit, joihin liittyy systeeminen riski

    - Tekoälymalli kuuluu tähän luokkaan, jos se käyttää laskentamallia 10^25 FLOPs eli suurta laskentatehoa tai jos Euroopan komissio katsoo tekoälymallin sisältävän systeemisiä riskejä perustuen muihin tekijöihin, esimerkiksi parametrien, autonomisuuden tai käyttäjämäärän perusteella. (Teknologiateollisuus ry 2025)

Kaikkiin yleiskäyttöisiin tekoälymalleihin kohdistuu vaatimuksia teknisen dokumentoinnin, jatkotarjoajan informoinnin sekä tekijänoikeuksien osalta. Systeemisen riskin malleille asetetaan myös lisävaatimuksia, joita on mallin arviointi, vakavien vaaratilanteiden seuraaminen sekä niistä raportoiminen ja riittävän kyberturvallisuustason varmistaminen mallille sekä sen fyysiselle infrastruktuurille. (Teknologiateollisuus ry 2024)

2.5 Vinoumat

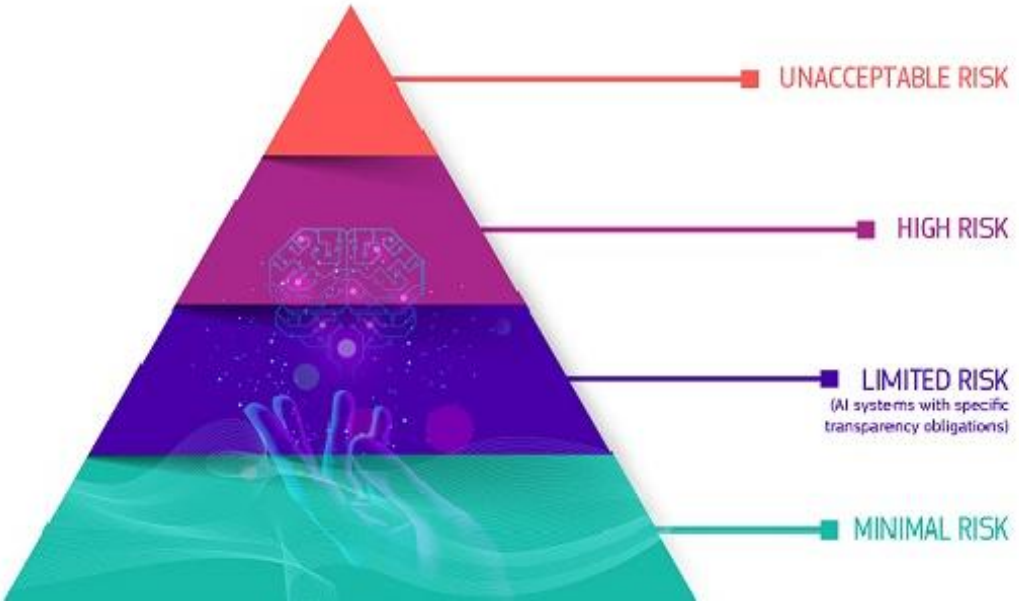
Datan vinoumalla tarkoitetaan otantaan tai testaukseen sisältyvää systemaattista virhettä, joka on seuraus siitä, kun valitaan tai voimistetaan yhtä tulosta tai vastausta muiden sijasta. Tämä on tilasto- ja tietojenkäsittelytieteellinen tapahtuma, joka aiheutuu tahattomasti tai kehitysprosessissa tahallisesti testimielessä. Tämänlainen vinouma voidaan aiheuttaa myös pahantahtoisin syin. Vinouma voidaan määritellä myös ennakkoasenteena, joka suosii tai vastustaa epäoikeudenmukaisesti tiettyä asiaa, henkilöä tai ryhmää verrattuna toiseen. Tällä viitataan ihmisen tai ihmisryhmän ominaisuuksiin, jotka heijastuvat järjestelmän tuottamaan tai sen käyttämään dataan joko tahallisesti tai tahattomasti. (Suomi.fi 2023)

Vinoumia syntyy, kun data on historiallista eli se sisältää sukupuoleen tai vähemmistöryhmiin liittyviä asenteita ja kuvaa mennyttä aikaa. Mikäli pitkäaikaisia vinoumia sisältävää dataa käytetään nykyajan järjestelmissä tuloksena, on jatkuva samojen vinoumien elinkaari yhteiskunnassa.

Vinoumia syntyy myös liian vähäisen datan, keräys- ja valintavinoumien sekä algoritmisen mallin koulutusvaiheen suunnitteluvirheiden takia. (Suomi.fi 2023)

3 TEKOÄLYJÄRJESTELMIEN RISKILUOKITTELU

Tekoälysäädös luokittelee tekoälyjärjestelmät neljään eri riskiluokkaan. Kuvassa 3 on esitettynä nämä riskiluokat pyramidimuodossa. Pyramidin huipulla on korkean riskin järjestelmät, joita on suhteessa vähiten, mutta niihin kohdistuvat vaatimukset ovat kaikista tiukimpia. Minimaalisen riskin järjestelmiä taas on määrällisesti eniten, ja niihin asetetut vaatimukset ovat pieniä.



KUVA 3. Tekoälyjärjestelmien riskiluokittelu (Euroopan unioni 2025)

3.1 Kestämätön riski – kielletyt käyttötapaukset

Tekoälysäädöstä on 1.2.2025 alkaen alettu soveltamaan kiellettyjen käyttötapausten osalta, joiden riski luokitellaan kestämättömäksi. Riski on kestämätön, kun se uhkaa ihmisen perusoikeuksia ja turvallisuutta. EU on sitoutunut periaatteillaan suojelemaan kansalaisiaan, joten näiden käyttötapausten kieltäminen on ehdottoman tärkeää.

Tekoälysäädöksessä kielletään seuraavat kahdeksan tekoälyn käyttötapausta (EU, 2024/1689):

- tekoälyjärjestelmät, jotka perustuvat manipulointiin ja petokseen aiheuttamalla merkittävää haittaa pyrkiessään vaikuttamaan ihmisten päätöksentekoon ilman, että päätöksentekoa on havaittu tietoisesti

- tekoälyjärjestelmät, jotka hyödyntävät ryhmän tai henkilön haavoittuvuuksia siten, että se aiheuttaa merkittävää haittaa

- tekoälyjärjestelmät, jotka arvioivat henkilöä sosiaalisen käyttäytymisensä tai henkilökohtaisten ominaisuuksien ja luonteenpiirteiden perusteella siten, että se johtaa perusteettomaan epäoikeudenmukaiseen kohteluun eli ns. sosiaalinen pisteytys

- tekoälyjärjestelmät, jotka arvioivat riskiä syyllistyä rikokseen pelkän henkilön profiloinnin tai ominaisuuksien perusteella

- tekoälyjärjestelmät, jotka luovat tai laajentavat kasvojentunnistustietokantoja internetistä tai esimerkiksi valvontakameramateriaalista poimittujen kuvien avulla

- tekoälyjärjestelmät, jotka pyrkivät tunteiden päättelyyn työpaikoilla ja oppilaitoksissa (pl. turvallisuuteen tai lääketieteeseen perustuvat syyt)

- biometriset luokittelujärjestelmät, jotka luokittelevat henkilöitä arkaluonteisten tietojen, kuten rodun, poliittisen mielipiteen tai uskonnollisen vakaumuksen perusteella.

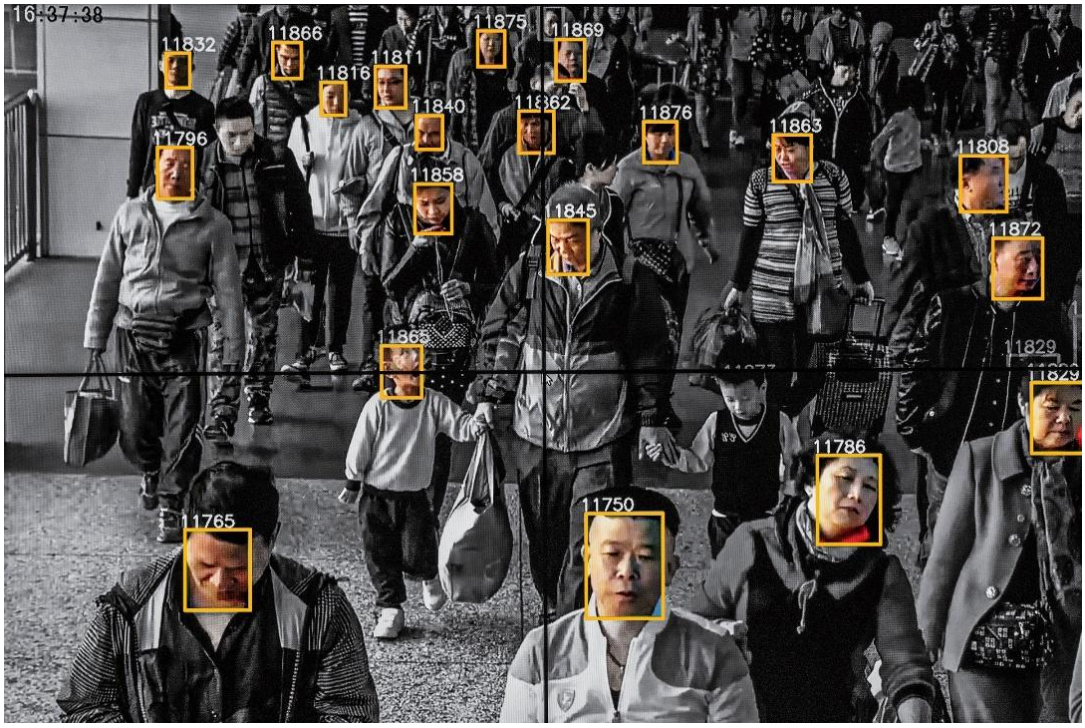
- julkisilla paikoilla reaaliaikaista biometristä etätunnistusta hyödyntävät järjestelmät (pl. tarkoin rajatut välttämättömät tapaukset, kuten kadonneiden henkilöiden tai ihmiskaupan uhrien etsintä, välittömän turvallisuusuhkan estäminen, vakavasta rikoksesta epäillyn tunnistaminen)

3.1.1 Esimerkkejä kielletyistä järjestelmistä

Sosiaalinen pisteytys (kuva 4.) ja ihmisten arviointi tekoälyjärjestelmän avulla on nostanut esiin monia yksityisyyteen ja perusoikeuksiin liittyviä kysymyksiä sekä huolta ihmisoikeuksien toteutumisen näkökulmasta. Esimerkiksi Kiinassa käytetään järjestelmiä, jotka arvioivat tekoälyn avulla kansalaisten kelpoisuutta yhteiskuntaan. Euroopassa vastaavia käytäntöjä ei tiedettävästi ole ollut käytössä, mutta tekoälyä on voitu hyödyntää esimerkiksi sosiaaliturvaan liittyvissä käsittelytoimenpiteissä ja joissakin maissa poliisiorganisaatioissa. Ihmisiä saa vakavien

rikosten tutkinnassa tunnistaa edelleen tekoälyjärjestelmien avulla, mutta näihin käytäntöihin liittyy tarkat vaatimukset.

Säädöksessä määritetään raamit tekoälyn hyödyntämiseen näillä sektoreilla ja pyritään luomaan turvaa perusoikeuksille kieltämällä sosiaaliseen pisteytykseen viittaavat valvontakäytänteet. (Harjumaa 2023)



KUVA 4. Sosiaalinen pisteytys tekoälyn avulla (EU Political Report 2023)

Järjestelmät, jotka voivat aiheuttaa vaaraa haavoittuvassa asemassa oleville kuuluvat kiellettyjen käytäntöjen listaan. Kiellettäviksi luokitellaan esimerkiksi lelut, jotka hyödyntävät tekoälyyn pohjautuvaa ääniohjausjärjestelmää ja voivat sillä kannustaa lasta vaaralliseen käytökseen. (Harjumaa 2023)

3.2 Suuri riski

Suuririskisiksi järjestelmiksi luetaan sellaiset järjestelmät, jotka voivat aiheuttaa vakavia riskejä terveydelle, turvallisuudelle tai perusoikeuksille. Niille asetetaan tiukkoja velvoitteita. (EU 2024/1689)

Suuririskisiä järjestelmiä ovat seuraavat:

1) Tekoälyjärjestelmä on suunniteltu käytettäväksi tuotteen turvakomponenttina tai on itse tuote, joka sisältyy unionin yhdenmukaistamislainsäädännön soveltamisalaan. (EU 2024/1689)

   Tuoteturvasäädöksen (EU) 2023/988 kautta tekoälysäädöksen soveltamisalaan tulevia tuotteita on esimerkiksi koneet, hissit, painelaitteet, henkilönsuojaimet sekä lääkinnälliset laitteet. (Teknologiateollisuus ry 2024)

2) Tekoälyjärjestelmät, jotka on tarkoitettu seuraaviin käyttötarkoituksiin ja esimerkit:

   - kriittisen infrastruktuurin turvakomponentit (esim. liikenne, sähkönjakelu ja vedenjakelu
   - tekoälypohjaiset turvakomponentit (esim. robottiavusteisessa kirurgiassa käytettävä tekoälysovellus)
   - oppilaitoksissa käytössä olevat tekoälyratkaisut, jotka voivat vaikuttaa koulutukseen ja työelämään pääsemiseen (esim. koetulosten pisteytys)
   - tekoälyratkaisut, joita käytetään työllistämiseen, henkilöstöhallintoon sekä itsenäiseen ammatinharjoittamiseen (esim. hakijoiden ansioluetteloiden tai työhakemusten lajitteluohjelmisto)
   - keskeisten yksityisten ja julkisten palvelujen tarjoamiseen käytettävät tietyt tekoälyratkaisut (esim. luottopisteytys, mahdollisuus saada lainaa evätään)
   - lainvalvonnassa käytettävät ihmisen perusoikeuksiin mahdollisesti vaikuttavat tekoälyratkaisut
   - muuttoliikkeen hallinta, turvapaikka-asiat ja rajavalvonta (esimerkiksi automatisoitu viisumihakemusten käsittely)
   - oikeudenhoito ja demokraattiset prosessit (esim. tuomioistuimien tekoälyratkaisut päätösten valmistelemiseksi)

3.2.1 Poikkeukset muissa käyttötapauksissa

Poikkeuksia on kuitenkin muutamia. Mikäli järjestelmä suorittaa suppeaa menettelytehtävää, parantaa aiemmin suoritettua ihmisen tuottamaa tulosta, jos järjestelmä havaitsee poikkeamia aiemmista päätöksentekotavoista tai jos järjestelmä suorittaa valmistelutehtävää eli esimerkiksi käsittelee tietoja. Mikäli järjestelmä poikkeaa edellä mainituilla tavoilla, voidaan se luokitella muuhun kuin suuren riskin järjestelmiin eikä vaatimuksia tarvitse täyttää. (Teknologiateollisuus ry 2024)

3.3 Suuririskisten järjestelmien vaatimukset

Ennen suuririskisen tekoälyjärjestelmän saattamista EU:n markkinoille tai sen käyttöönottoa muulla tavoin, tulee järjestelmän tarjoajan tehdä sille vaatimustenmukaisuuden arviointi.
Suuririskisen tekoälyjärjestelmän tarjoajan tulee varmistaa, että järjestelmä täyttää vaatimukset, joita on asetettu seitsemälle eri osa alueelle. (EU 2024/1689)

3.3.1 Riskinhallintajärjestelmä

Suuririskisille tekoälyjärjestelmille on perustettava ja ylläpidettävä riskinhallintajärjestelmää, joka kattaa koko järjestelmän elinkaaren. Järjestelmä toimii toistuvana prosessina, jossa riskien tunnistus, arviointi ja hallinta on jatkuvaa.
Tähän prosessiin kuuluu tunnettujen ja ennakoitavien riskien tunnistaminen ja analysointi sekä asianmukaisten riskienhallintatoimenpiteiden suunnittelu ja toteutus. (EU 2024/1689)

3.3.2 Data ja datanhallinta

Dataan ja datanhallintaan liittyy suuririskisten järjestelmien osalta useita vaatimuksia. Koulutus-, validointi- ja testausdatan hallinta on keskeinen asia järjestelmän luotettavuuden ja turvallisuuden varmistamiseksi ja niiden on täytettävä tietyt laatuvaatimukset.
Käytettävän datan tulee olla merkityksellistä ja mahdollisimman virheetöntä. On tärkeää tunnistaa ja korjata mahdolliset vinoumat, jotka voivat johtavaa syrjintään. (EU 2024/1689)

3.3.3 Tekninen dokumentaatio

Suuririskisen järjestelmän tekninen dokumentaatio tulee laatia ennen sen käyttöönottoa tai saattamista markkinoille. Dokumentaation tulee pysyä ajantasaisena ja siinä täytyy osoittaa järjestelmän vaatimustenmukaisuus. Viranomaisten tulee kyetä arvioimaan dokumentaation perusteella täyttääkö järjestelmä vaatimukset. (EU 2024/1689)

Tekninen dokumentaatio on yksityiskohtainen ja siihen tulee sisällyttää ainakin seuraavat asiat:

1. Yleinen kuvaus järjestelmästä sisältäen nämä tiedot:

    - käyttötarkoitus, tarjoajan nimi ja järjestelmän versio
    - tekoälyjärjestelmän vuorovaikutus muiden laitteiden tai ohjelmistojen mukaan lukien muiden tekoälyjärjestelmien kanssa
    - laitteistovaatimukset, käyttöohjeet sekä käyttöliittymän peruskuvaus
    - ohjelmistojen versiot ja versiopäivitysten vaatimukset
    - kuvaus muodoista, jossa järjestelmä käyttöönotetaan tai saatetaan markkinoille (laitteiston ohjelmistopaketit, ladattavat versiot tai sovellusrajapinnat)
    - kuvaus järjestelmän käyttöön tarkoitetusta laitteistosta
    - järjestelmän ollessa osa tuotetta, tulee tekniseen dokumentaatioon liittää kuva tai piirrokset, joista käy ilmi tämän tuotteen merkinnät, sisäinen kokoonpano ja ulkoiset ominaisuudet
    - käyttöliittymän peruskuvaus ja käyttöohjeet käyttöönottajalle

2. Yksityiskohtaiset tiedot järjestelmän osista ja sen kehittämisprosessista, sisältäen ainakin seuraavat tiedot:

    - järjestelmän kehityksessä käytetyt menetelmät
    - rakennespesifikaatiot
    - kuvaus järjestelmäarkkitehtuurista, jossa selitettynä ohjelmistokomponenttien keskinäinen vuorovaikutus
    - järjestelmässä käytetyt laskentaresurssit
    - käytettävät kyberturvallisuustoimenpiteet

Lisäksi tekniseen dokumentaatioon tulee sisällyttää:

- kuvaus järjestelmän suorituskykymittareiden asianmukaisuudesta
- luettelo sovelletuista yhdenmukaistetuista standardeista
- tarkka kuvaus luodusta riskienhallintajärjestelmästä
- jäljennös EU- vaatimustenmukaisuusvakuutuksesta

3.3.4 Tietojen säilyttäminen

Suuren riskin tekoälyjärjestelmissä on mahdollistettava tapahtumien eli niin sanottujen lokitietojen automaattinen tallentaminen koko järjestelmän käyttöiän ajan. Näiden tietojen säilyttämisellä voidaan tunnistaa sellaiset tapahtumat, jotka voisivat vaikuttaa terveyteen, turvallisuuteen tai perusoikeuksiin. Eli lokitietojen ollessa tallennettuna järjestelmään on nämä tapahtumat mahdollista jäljittää. (EU 2024/1689)

3.3.5 Avoimuus ja tietojen antaminen käyttöönottajille

Suuririskiset tekoälyjärjestelmät on kehitettävä ja suunniteltava tarpeeksi avoimiksi, jotta käyttöönottajilla on mahdollisuus tulkita ja hyödyntää niiden tuotoksia asianmukaisesti. Järjestelmien mukana tulee toimittaa paikkansapitävät käyttöohjeet, jotka ovat selkeät ja kattavat. (EU 2024/1689)

3.3.6 Ihmisen suorittama valvonta

Suuririskisten tekoälyjärjestelmien suunnittelu on toteutettava siten, että luonnollisilla henkilöillä on mahdollisuus valvoa niitä tehokkaasti. Valvonnan tulee minimoida terveydelle, turvallisuudelle tai perusoikeuksille aihetuvat riskit, joita voi syntyä järjestelmää käytettäessä oikein tai ennakoitavissa olevissa väärinkäytön mahdollisuuksissa.

Valvontatoimenpiteiden tulee olla suhteutettuna järjestelmän riskeihin, itsenäisyyden tasoon ja käyttöympäristöön. Ne voidaan toteuttaa joko järjestelmässä sisäisesti ennen sen markkinoille saattamista tai käyttöönottajan toimesta käyttöönoton yhteydessä.

Valvontatehtävää suorittavan henkilön on ymmärrettävä järjestelmän valmiudet ja rajoitukset sekä havaita ja reagoida sen toimintahäiriöihin. Valvonnassa tulee myös pysyä tietoisena ja huomioida, ettei synny ns. automaatiovinoumaa eli taipumusta luottaa liiallisesti tekoälyjärjestelmän antamiin tuloksiin. (EU 2024/1689)

3.3.7 Tarkkuus, vakaus ja kyberturvallisuus

Suuririskisten tekoälyjärjestelmien suunnittelu ja kehitys tulee toteuttaa siten, että ne ovat tarkkoja, vakaita ja kyberturvallisia koko elinkaarensa ajan. Järjestelmien suorituskykyä tulee arvioida asianmukaisilla mittareilla, joita voidaan kehittää yhteistyössä esimerkiksi asiantuntijoiden ja viranomaisten kanssa.
Järjestelmien on oltava mahdollisimman sietokykyisiä virheille, vioille ja epäjohdonmukaisuuksille, joita esiintyy järjestelmässä tai sen toimintaympäristössä.

Kyberturvallisuuden osalta suuririskisten järjestelmien tulee olla suojattuja ulkopuolisilta tahoilta, jotka voivat yrittää muuttaa järjestelmän toimintaa hyödyntämällä sen heikkouksia. Kyberturvallisuus on varmistettava teknisillä ratkaisuilla, jotka vastaavat niihin mahdollisesti kohdistuvia riskejä ja toimintaympäristön vaatimuksia. (EU 2024/1689)

3.4 Rajoittunut riski

Rajoittuneen riskin sisältäville järjestelmille asetetaan tiettyjä avoimuusvaatimuksia. Rajoittuneen riskin sisältäviä järjestelmiä ovat generatiivista tekoälyä hyödyntävät järjestelmät, esimerkiksi chatbotit. Ihmisen on tiedettävä kommunikoivansa tekoälyjärjestelmän kanssa ja pyrkimyksenä on välttää manipulaatiota ja huijauksia.
Tekoälyn luoma synteettinen ääni, kuva ja video on merkittävä esimerkiksi vesileimalla koneen tuotokseksi eli siitä on oltava havaittavissa, että se on tekoälyn luomaa eikä aitoa materiaalia. Mikäli tuotetaan deepfakea eli syvävääreennöstä hyödyntävää materiaalia on senkin käytävä ilmi tuotoksesta. (Teknologiateollisuus ry 2024)

3.5 Minimaalinen riski

Minimaalisen riskin järjestelmiksi luetaan esimerkiksi videopelit ja roskapostisuodattimet, näihin säädös ei aseta erillisiä velvoitteita. Asetuksen alaisuuteen eivät myöskään kuulu tieteelliseen tutkimus- ja kehityskäyttöön suunnitellut järjestelmät ja mallit, puolustukselliseen, sotilaalliseen tai kansallisen turvallisuuden

käyttöön suunnitellut järjestelmät ja luonnolliset henkilöt, jotka käyttävät järjestelmää vain henkilökohtaisiin tarkoituksiin.

4 TEKOÄLYN STANDARDOINTI

Tekoälyn kehittämiseen liittyy sääntelyn lisäksi standardointia, joka on merkittävässä roolissa lainsäädännön toimeenpanemiseksi. Kansainvälisesti tekoälyn standardointi on aloitettu vuonna 2018, jolloin SR 315 eli eri alojen asiantuntijoista koostuva kansallinen standardointiryhmä aloitti myös toimintansa. Tekoälyn standardeihin sisältyy viitekehysstandardit, yleiskatsaus, termistö, turvallisuus, laatu ja eettisyys. Eurooppalainen standardointi mukailee EU:n lainsäädäntöä käytäntöjä, periaatteita ja arvoja. Standardit helpottavat lainsäädännön noudattamista sekä yritysten toimintaa. Lisäksi standardoinnilla voidaan auttaa merkittävästi yhtenäisen terminologian luomisessa ja vakiinnuttamisessa. (Suomen Standardisoimisliitto SFS n.d.)

Standardien avulla muutetaan asetuksessa määritellyt vaatimukset konkreettisiksi toimenpiteiksi. Niissä voidaan esimerkiksi määritellä, mitä tilastollisia ominaisuuksia datasta tulisi mitata ja minkälaisissa yhteyksissä. Tekoälyä koskevat standardihankkeet ovat vielä keskeneräisiä ja verrattuna moniin muihin aloihin todella kehityksen alkuvaiheessa. Tekoälysäädöksessä asiat ovat esitetty melko yleisellä tasolla, jättäen varaa yksityiskohtien täydennykseen standardien avuin. (Pouget & Zuhdi 2024)

Standardeilla on merkittävä rooli tekoälyasetuksen myötä ohjata sitä, miten tekoälyn kanssa toimitaan. Standardien avulla vaikutetaan myös siihen, miten tekoälyyn suhtaudutaan ja mitä pidetään hyväksyttynä tekoälyjärjestelmissä ja niitä hyödyntävien organisaatioiden toiminnassa tulevaisuudessa. Standardointiryhmillä on tällä hetkellä työn alla kymmenen asetuksen kanssa harmonisoitua eli yhdenmukaista standardia, joiden odotetaan valmistuvan syksyllä 2026. Lisäksi kansainvälinen standardointijärjestö ISO on kehittämässä standardeja tekoälylle. (Reivo 2025)

Euroopan komissio arvioi ja julkaisee standardointijärjestöjen ehdottamat standardit, jotka pääosin keskittyvät suuririskisiin tekoälyjärjestelmiin. Standardien

käyttö antaa suuririskisen järjestelmän tarjoajalle oletuksen siitä, että heidän järjestelmänsä on sääntelyn mukainen. Standardien tulisi olla sovellettavissa eri toimialoilla ja olla yhtenäisiä sekä täydentää toisiaan. (Euroopan komissio 2024)

Osa-alueet, joille EU:n asetus pyytää standardisointia:

- riskienhallinta
- datan hallinta ja laatu
- tietojen säilytys
- läpinäkyvyys
- ihmisen suorittama valvonta
- tarkkuus
- vakaus
- kyberturvallisuus
- laadunhallinta
- vaatimustenmukaisuuden arviointi

Säädös asettaa vaatimuksena esimerkiksi riskienhallintajärjestelmän luomisen tekoälyjärjestelmälle. Riskienhallintajärjestelmän sekä muiden vaatimusten toteuttamiseen ohjeistusta annetaan standardien kautta. Euroopassa standardeja kehittää standardointijärjestö CEN-CENELEC. Nämä toimijat kehittävät standardeja yhdessä kansainvälisen standardointijärjestö ISO:n sekä kansainvälisen sähköteknisen komission IEC:n kanssa. (Pouget & Zuhdi 2024)

CEN-CENELEC järjestön perustaman teknisen komitean JTC 21:n tavoitteena on vastata eurooppalaisen markkinan tarpeisiin liittyen tekoälyn standardointiin, tukea EU-lainsäädäntöä, kehittää harmonisoituja standardeja säädöksen vaatimalla tavalla ja tarjota ohjeistusta muille toimijoille. Tärkeimpiä asetusta tukevia standardeja, joita järjestössä kehitetään ovat tekoälyn luotettavuuskehys, riskien- ja laadunhallintajärjestelmät sekä vaatimustenmukaisuuden arviointi. (CEN-CENELEC n.d)

Järjestö haluaa myös tehdä yhteistyötä muiden standardointijärjestöjen sekä sidosryhmien kanssa. Laajalla yhteistyöllä lisätään tietoisuutta standardoinnin hyödyistä ja kerätään eri toimialojen näkemyksiä. (CEN-CENELEC 2024)

Tekoälyä koskeva SFS-ISO/IEC 42001 on tekoälyn hallintajärjestelmän käsittävä standardi. Standardin avulla voidaan kehittää turvallisia ja vastuullisia tekoälyjärjestelmiä. Standardin tavoitteet ovat tiivistettynä seuraavat:

- edistää luotettavien, avoimien ja vastuullisten tekoälyjärjestelmien kehittämistä
- kunnioittaa eettisiä periaatteita ja yksityisyyttä
- auttaa organisaatioita tunnistamaan tekoälyn käyttöönottamiseen liittyviä riskejä
- noudattaa sääntelyvaatimuksia
- lisätä luottamusta tekoälyn hallintaan, organisaatioita kannustetaan laittamaan ihmisten hyvinvointi ja turvallisuus sekä käyttäjäkokemus etusijalle tekoälyjärjestelmiä suunniteltaessa (Brewer 2023)

Tämä standardi voi auttaa yrityksiä täyttämään tekoälysäädöksen vaatimukset, koska standardissa painotetaan samoja vaatimuksia kuin säädöksessä. Se tarjoaa menetelmiä eettisten vaikutusten arviointiin, datanhallintaan sekä suuren riskin järjestelmien tunnistamiseen. Standardi korostaa säädöksen edellyttämää tekoälyjärjestelmien läpinäkyvyyttä ja vastuullisuutta. (Krepki 2024)

5 SÄÄNTELYN TUOMAT HAASTEET JA MAHDOLLISUUDET

Tässä kappaleessa käydään läpi minkälaisia mahdollisuuksia ja haasteita tekoälysäädös tuo mukanaan. Lainsäädännön tuomat tiukat vaatimukset voivat estää erityisesti pieniä toimijoita kehittämästä ja ottamasta käyttöön tekoälyjärjestelmiä korkeiden vaatimusten takia. Tämän lisäksi monet suuret yritykset kuten Meta, Apple ja Google ovat kieltäytyneet tuomasta omia tekoälymallejaan EU:n markkinoille epämääräisen digisääntelyn takia. Varovaisuus tekoälyjärjestelmien tuomisesta EU:n markkinoille selittyy myös sääntelyn rikkomisesta seuraavista sakoista.

Kysymys siitä, jääkö Eurooppa tekoälykehityksen ulkopuolelle on monimutkainen. On mahdollista, että kehityksestä jäädään jälkeen, mutta myös kehitys itsessään voi hidastua, vaikka se tällä hetkellä onkin hyvin nopeaa. (Hallamaa 2024)

Näiden kehitykseen liittyvien haasteiden lisäksi säädöksen sisällössä on havaittu myös joitain aukkoja ja epäselvyyksiä. Säädös tunnistaa vain välittömiä ja ennakoitavissa olevia haittoja tekoälyjärjestelmien ollessa luokiteltuna riskiperusteisesti. Eli niin sanotut algoritmiset haitat, joiden ennakointi ei ole helppoa jäävät säädöksessä huomiotta. Säädöksessä tunnistetaan systeemiset riskit, mutta niiden rajoittamiseen liittyvät toimenpiteet ovat melko olemattomia ja vaatimukset kohdentuvat vain pieneen osaan tekoälymalleista. Sääntely jää siis joiltain osin vaillinaiseksi. (Lepinkäinen 2024)

Haasteiden lisäksi tuo sääntely mukanaan myös hyötyjä ja mahdollisuuksia. EU:n on mahdollista saavuttaa globaali johtoasema eettisen tekoälyn kehityksessä ja samalla näyttää esimerkkiä muille alueille asettamalla korkeat turvallisuus- ja eettisyysstandardit. Tekoälysäädöksellä tuodaan yksilöille turvaa ja luottamusta tekoälyyn. Säädös velvoittaa tekoälyn käytön läpinäkyvyyteen eli tällöin käyttäjät ovat tietoisia tekoälyn tekemistä päätöksistä prosessissa. (Euroopan komissio 2024)

Säädöksen avulla saadaan tasaiset kilpailu- ja toimintaolosuhteet, kun kaikkien EU:n markkinoille järjestelmiään tuovien yritysten on noudatettava sitä. (Ditsche & Mikhaylenko 2023)

6 VAIKUTUKSET TEKNOLOGIATEOLLISUUDEN ALAN YRITYKSIIN

Tässä osiossa käydään läpi säädöksen vaikutuksia teknologiateollisuuden alojen yrityksiin. Säädös asettaa vaatimuksia monelle eri osa-alueelle ja siten pakottaa yritykset pohtimaan tekoälyn käyttöä yrityksessä. Tekoälyn sääntely tulee vaikuttamaan monien eri alojen yritysten toimintaan. Säännösten tuomat vaikutukset ja niihin varautuminen voivat olla aikaa vieviä prosesseja ja tarvita erillistä koulutusta. Voidaan kuitenkin huomata se, että monet säädöksen tuomat vaatimukset ovat kohdennettu ns. julkisen vallan käyttäjiin eli esimerkiksi valtion hallintoelimiin ja tuomioistuimiin. (Teknologiateollisuus ry 2025)

Säädös astuu voimaan täysimääräisesti vasta vuonna 2026, joten lopulliset vaikutukset voidaan nähdä vasta myöhemmin. Kuitenkin jo nyt vaikutuksia voidaan arvioida ja niihin voidaan alkaa valmistautumaan.

Teollisuuden tuotantoprosesseissa käytettävät järjestelmät eivät säädöksen mukaan todennäköisesti ole suuririskisiä. Säädökseen kuitenkin kytkeytyy EU:n tuoteturvavaatimukset, joiden tuoteryhmiin sovelletaan suuririskisten tekoälyjärjestelmien vaatimuksia tietyin ehdoin. (Mikkilä 2024)

6.1 Turvakomponentit

Järjestelmä voidaan luokitella suuririskiseksi, mikäli teollisuusyritys hyödyntää tekoälyjärjestelmää tuoteturvasääntelyn piiriin kuuluvan tuotteensa turvakomponenttina. Tässä tapauksessa sen tulee myös olla vaatimustenmukainen. (Mikkilä 2024)

Turvallisuuskomponentteina käytettävät tekoälyjärjestelmät kriittisen infrastruktuurin, kuten tieliikenteessä sekä veden ja sähkön jakelussa käytettävät järjestelmät ovat suuririskisiä. Näitä voivat olla esimerkiksi hälytyslaitteet, vedenpainetta valvovat järjestelmät tai palohälytysjärjestelmän ohjausjärjestelmät. Näiden tekoälyjärjestelmien vikaantuminen tai toimintahäiriöt voivat aiheuttaa mittavia riskejä ihmisen hengelle ja terveydelle sekä yhteiskunnalliseen ja taloudelliseen toimintaan. (EU 2024/1689)

Yhtenä esimerkkinä tästä käyttötapauksesta nousee autoteollisuus ja autonomisten ja automatisoitujen ajoneuvojen kehittäminen. Tekoälyä käytetään jo laajasti autoalalla, sen avulla voidaan parantaa ajoneuvojen turvallisuutta ja älykkyyttä. Lisäksi tekoälyn avulla voidaan seurata auton kuljettajan vireystilaa ja mahdollisesti näin ehkäistä tapaturmia. Tekoälyn käyttö autoalalla voi myös aiheuttaa merkittäviä riskejä, joihin säädöksellä pyritään vastaamaan. Suurimmaksi osaksi autonomiset ja avustavat ajotoiminnot tulevat kuulumaan suuren riskin luokkaan, sillä ne vaikuttavat ajoturvallisuuteen merkittävästi. Tekoälysäädös toimii yleisenä sääntelykehyksenä, mutta jo autoalalle kohdistetut lainsäädännöt tarkentavat vaatimuksia. (Kahl 2025)

6.2 Yleiskäyttöiset tekoälymallit

Teollisuusyrityksen, joka integroi tekoälyjärjestelmänsä yleiskäyttöiseen tekoälymalliin tulee varmistaa toimittajan kanssa tekoälymallin riskiluokitus ja vaatimustenmukaisuus. Yrityksen hienosäätäessä toisen toimijan markkinoille tuomaa yleiskäyttöistä mallia, tulee yrityksestä sen mallin tarjoaja, johon sovelletaan säädöksen velvoitteita. (Mikkilä 2024)

6.3 HR-järjestelmät

Yritysten käyttämät henkilöstöhallinnon ja rekrytoinnin järjestelmät voivat olla suuririskisiä, joten vaatimustenmukaisuudesta tulee varmistua. (Mikkilä 2024)

Tekoälyjärjestelmät, joita hyödynnetään ihmisten työllistämisessä ja henkilöstöhallinnossa niiden päätösten tekemiseen, joiden vaikutus kohdistuu työsuhteen ehtoihin, uralla etenemisen ja työsuhteen päättämisen ehtoihin, työtehtävien jakamiseen henkilön käyttäytymisen tai persoonallisuuspiirteiden perusteella tai joita käytetään henkilöiden seurantaan tai arviointiin.

Tämänkaltaiset järjestelmät voivat merkittävästi vaikuttaa yksilön uranäkymiin, toimeentuloon ja työntekijälle kuuluviin oikeuksiin. Näiden järjestelmien tulee täyttää säädöksessä asetetut tiukat vaatimukset eli läpinäkyvyyden varmistaminen, ihmisen valvonnan mahdollisuus ja riskianalyysien suorittaminen. (EU 2024/1689)

Esimerkiksi teknologiayhtiö IBM Systems on tutkinut vinoumien vaikutusta tasa-arvoon. Tekoäly käyttää tietoperustanaan nykyistä maailmaa kuvaavaa tietoa sisältäen myös olemassa olevat epätasa-arvoisuudet. Naiset ovat useammin osa-aikatyössä kuin miehet, joten tekoäly päättelee miesten olevan parempia työntekijöitä ja soveltuvan kokoaikaisiin työtehtäviin naisia paremmin. (Ulkoministeriö 2023)

6.4 Tekoälyä kehittävät yritykset

Säädöksen suurimmat vaikutukset teknologiateollisuuden alalla kohdistuvat tekoälyä kehittäviin IT-yrityksiin. Näiden yritysten vastuulla on varmistaa asiakkaan kanssa järjestelmän riskiluokitus ja mihin käyttöön se tulee. Lisäksi tarvittaessa tulee varmistaa myös järjestelmän vaatimustenmukaisuus.

Eri viranomaisia palvelevien yritysten tulee olla erityisen tarkkana, sillä suuri osa kielletyistä ja suuririskisistä järjestelmistä koskee julkista valtaa. Eurooppalaiset startup- ja kasvuyritykset saattavat jäädä jälkeen sellaisten alueiden kilpailijoille, joille kohdistuu suhteessa kevyempää säätelyä. On myös mahdollista, että EU:n ulkopuoliset tekoälyjärjestelmien tarjoajat lykkäävät tuotteidensa tuomista Eurooppaan tiukan sääntelyn vuoksi. Tämän seurauksena teollisuusyritysten mahdollisuus käyttää uusimpia sovelluksia pienenisi ja tekoälyn hyödyt leviäisivät hitaammin Eurooppaan. (Mikkilä 2024)

Tekoälylainsäädännöllä kuitenkin halutaan tukea innovointia ja startup-yrityksiä. Yrityksillä on mahdollisuus kehittää ja testata yleiskäyttöisiä tekoälymalleja ennen niiden saattamista markkinoille. Kansallisten viranomaisten tulee tarjota yrityksille testiympäristö, joka mukailee järjestelmän todellista käyttöä. (Euroopan parlamentti 2025)

6.5 Valmistautuminen ja koulutus

Asetuksen mukaan jokaisen tekoälyä hyödyntävän tai tarjoavan yrityksen tai organisaation tulee varmistaa henkilöstön riittävä tekoälylukutaito. Tällä tarkoitetaan kykyä ymmärtää eettiset ja tehokkaat tavat tekoälyn hyödyntämiseen. (EU 2024/1689)

Tekoälylukutaidon tärkeys korostuu, kun lähes jokaisessa työpaikassa tai oppilaitoksessa tekoälyjärjestelmiä hyödynnetään tavalla tai toisella. Taidon parantamiseksi on olemassa paljon erilaisia koulutuksia, joissa läpikäydään yleisesti tekoälyä, sen sääntelyä ja eettisyyttä.

Yrityksissä sääntelyn tuomiin vaikutuksiin voidaan valmistautua myös eri järjestelmien avuin. Sääntelyn ymmärtämiseksi ja sen noudattamiseksi Teknologiateollisuus ry suosittelee jäsenilleen Entries- työkalua. Sen avulla yritykset voivat navigoida säädöstä ja tuottaa personoidun koosteen heitä koskettavista säädöksen vaatimuksista. (Teknologiateollisuus ry 2025)

6.6 Tekoälyn sääntelyn testiympäristöt

Säädös määrää, että jäsenvaltioiden on perustettava tekoälyn testiympäristö viimeistään 2. elokuuta 2026. Nämä testiympäristöt eli niin sanotut sääntelyhiekkalaatikot tarjoavat valvotun ympäristön, jossa on mahdollisuus turvallisesti kehittää ja testata järjestelmää ennen virallista käyttöönottoa.
Sääntelyhiekkalaatikoilla pyritään edistämään parhaiden käytäntöjen jakamista niihin osallistuvien viranomaisten kanssa, edistää ja vauhdittaa startup ja pk-yritysten tekoälyjärjestelmien markkinoille pääsyä ja edistää näyttöön perustuvaa sääntelyyn liittyvää oppimista. (EU 2024/1689)

7 POHDINTA

Opinnäytetyön tavoitteena oli tutkia EU:n tekoälysäädöksen sisältöä ja selvittää kuinka se vaikuttaa teknologiateollisuuden yritysten toimintaan. Työn tuloksena saatiin yhteenveto säädöksen sisällöstä ja sen oleellisimmista vaikutuksista teknologiateollisuuteen.

Tutkimusta olisi voinut kehittää esimerkiksi eri yrityksiin kohdennetuilla kyselyillä, joiden avulla olisi saatu enemmän konkreettisia esimerkkejä säädöksen tuomista vaikutuksista. Työ kuitenkin haluttiin toteuttaa internet lähteisiin painottuvalla kirjallisuustutkimuksena. Opinnäytetyössä hyödynnetty lähdeaineisto on julkaistu pääosin 2020-luvulla, mikä takaa ajantasaisuuden ja mahdollisimman tuoreet tiedot.

Työssä olisi voinut käsitellä myös muita tekoälyjärjestelmien kehitykseen vaikuttavia EU-säädöksiä, mutta rajaus lopulta tehtiin vain tekoälysäädöksen sisältöön. Rajauksella kuitenkin saatiin aikaan juuri tähän säädökseen kohdennettu tietopaketti ja tutkimus.

Tekoälysäädös luo hyvät raamit turvallisen tekoälyn kehitykselle ja varmistamalla eettiset käytännöt turvataan niin yksilöiden kuin yritysten toimintaa. Tekoäly on kehittynyt viimeisten vuosien aikana nopeasti ja se tuo mukanaan paljon kysymyksiä liittyen eettisyyteen ja turvallisuuteen. Lainsäädännön tarve on välttämätön, jotta läpinäkyvyys tekoälyn kehittämisessä säilyy ja mahdollisia väärinkäytöksiä pystytään vähentämään.

Vastuullisten järjestelmien kehittäminen vaatii jatkuvaa arviointia sekä algoritmien päivitystä, jotta epätasa-arvoon johtavat vinoumat voitaisiin estää. Tulevaisuudessa tekoälyratkaisujen avulla voidaan tehdä päätöksiä esimerkiksi terveydenhuollossa sekä opiskelijavalinnoissa. Sääntelyn ansiosta ratkaisut tulee toteuttaa luotettavasti ja Euroopan unionin arvokysymykset huomioiden. EU:n tekoälysäädöksen voidaan todeta olevan merkittävä askel kohti turvallisempaa ja vastuullisempaa tekoälyn kehittämistä.

LÄHTEET

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689 tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös). Euroopan unionin virallinen lehti 12.7.2024. Viitattu 27.1.2025. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32024R1689

Teknologiateollisuus ry. 2025. Tekoälyasetus – tekoälyjärjestelmien ja yleiskäyttöisten tekoälymallien turvallisuussäädös. Verkkosivu. Viitattu 1.2.2025. https://teknologiateollisuus.fi/jasenille/tietopankki/digitalisaatio-ja-tekoaly/tekoalyasetus/

Euroopan unioni. 2024. Verkkosivu. Viitattu 1.2.2025. https://digital-strategy.ec.europa.eu/fi/policies/regulatory-framework-ai

Euroopan unioni. 2025. Yleiskäyttöiset tekoälymallit tekoälysäädöksessä. Verkkosivu. Viitattu 1.2.2025. https://digital-strategy.ec.europa.eu/fi/faqs/general-purpose-ai-models-ai-act-questions-answers

Valtiovarainministeriö. EU:n digisäädökset, n.d. Verkkosivu. Viitattu 12.3.2025. https://vm.fi/eu-n-digisaadokset

Työ- ja elinkeinoministeriö. n.d. EU:n tekoälyasetuksen kansallinen toimeenpano. Verkkosivu. Viitattu 20.3.2025. https://tem.fi/tekoalyasetus

Työ- ja elinkeinoministeriö. 2025. EU:n tekoälyasetus: tekoälykäytäntöjen kiellot astuvat voimaan 2.2.2025. Verkkosivu. Viitattu 20.3.2025. https://tem.fi/-/eu-n-tekoalyasetus-tekoalykaytantojen-kiellot-astuvat-voimaan-2.2.2025

Suomi.fi kehittäjille. 2023. Tekoälyn vastuullinen hyödyntäminen. Verkkosivu. Viitattu 25.3.2025. https://kehittajille.suomi.fi/oppaat/vastuullinen-tekoaly/maarittele-datapolitiikka/vinoumat-on-tunnistettava-ihmisvoimin

Euroopan komissio. 2024. Tekoäly – kysymyksiä ja vastauksia. Verkkosivu. Viitattu 25.3.3035. https://ec.europa.eu/commission/presscorner/detail/fi/qanda_21_1683

Pouget & Zuhdi, 2024. AI and Product Safety Standards Under the EU AI Act. Verkkosivu. Viitattu 27.3.2025. https://carnegieendowment.org/research/2024/03/ai-and-product-safety-standards-under-the-eu-ai-act?lang=en

SESKO ry. n.d. Mitä SESKO tekee? Verkkosivu. Viitattu 27.3.2025. https://sesko.fi/sesko_ry/

Suomen Standardisoimisliitto SFS. n.d. SFS/SR 315 Tekoäly. Verkkosivu. Viitattu 27.3.2025. https://sfs.fi/osallistu-ja-vaikuta/standardointiryhmat/tekoaly/

Kahl, T. 2025. AI Act and the Automotive Industry – Where does the road lead? Taylor Wessing. Verkkosivu. Viitattu 28.3.2025. https://www.taylorwessing.com/en/insights-and-events/insights/2025/03/ai-act-and-the-automotive-industry

Fscom. 2024. The EU AI Act: proactivity is crucial for financial institutions to meet key deadlines. Verkkosivu. Viitattu 31.3.2025. https://fscom.co/ie/blog/the-eu-ai-act-proactivity-is-crucial-for-financial-institutions-to-meet-key-deadlines/

Euroopan unionin neuvosto. 2024. Artificial intelligence. Verkkosivu. Viitattu 31.3.2025. https://www.consilium.europa.eu/fi/policies/artificial-intelligence/#what

Hallamaa, T. 2024. Tuleeko EU:sta tekoälyn takapajula? Verkkosivu. Viitattu 31.3.2025. https://yle.fi/a/74-20102412

Kivimäki, M. 2025. Uusi tekoälysääntely on jo ovella – näin se vaikuttaa EU:n yrityksiin ja ihmisiin. Verkkosivu. Luettu 31.3.2025. https://www.tivi.fi/uutiset/uusi-tekoalysaantely-on-jo-ovella-nain-se-vaikuttaa-eun-yrityksiin-ja-ihmisiin/9463939f-e410-4da4-b9a6-79c1bbfb999e

Mikkilä, J. 2024. Näin EU:n tekoälysääntely vaikuttaa teknologiateollisuuteen – kansallisessa toimeenpanossa ei varaa harha-askeliin. Verkkosivu. Viitattu 1.4.2025. https://teknologiateollisuus.fi/nain-eun-tekoalysaantely-vaikuttaa-teknologiateollisuuteen-kansallisessa-toimeenpanossa-ei-varaa-harha-askeliin/

Euroopan parlamentti. 2025. EU:n tekoälysäädös on ensimmäinen laatuaan. Verkkosivu. Viitattu 1.4.2025. https://www.europarl.europa.eu/topics/fi/article/20230601STO93804/eu-n-tekoalysaados-on-ensimmainen-laatuaan

Traficom. 2024. EU:n digi- ja datasääntely pähkinänkuoressa. Verkkosivu. Luettu 2.4.2025. https://www.traficom.fi/fi/viestinta/datatalous-ja-digipalvelut/eun-digi-ja-datasaantely-pahkinankuoressa

Ulkoministeriö. 2024. Teknologia-alan johtaja - tekoälyn vinoumia voidaan korjata tasa-arvoisiksi. Verkkosivu. Viitattu 2.4.2025. https://um.fi/uutiset/-/asset_publisher/GRSnUwaHDPv5/content/teknologia-alan-johtaja-tekoalyn-vinoumia-voidaan-korjata-tasa-arvoisiksi-/35732

Helakallio A. 2025. Tekoälysäädös hämmentää – hurjiakin väärinkäsityksiä on ollut. Verkkosivu. Luettu. 2.4.2025. https://www.tivi.fi/uutiset/tekoalysaados-hammentaa-hurjiakin-vaarinkasityksia-on-ollut/b9a34e63-fe93-41bd-bd2c-3656a06e3e2a

Lepinkäinen N. 2024. Algoritmiset haitat - Tekoälyn riskit ja sääntelyn haasteet kiihtyvässä yhteiskunnassa. Väitöskirja. Viitattu 7.4.2025. https://www.utupub.fi/handle/10024/178882

Euroopan unioni. 2024. Ethics guidelines for trustworthy AI. Verkkosivusto. Viitattu 11.4.2025. https://digital-strategy.ec.europa.eu/fi/library/ethics-guidelines-trustworthy-ai

Ditsche, J., & Mikhaylenko, M. 2023. European AI Act: Opportunities and challenges. Verkkosivu. Viitattu 11.4.2025. https://www.rolandberger.com/en/Insights/Publications/European-AI-Act-Opportunities-and-challenges.html

Harjumaa M. 2023. Näin EU aikoo rajoittaa tekoälyn käyttämistä: muun muassa deepfake-kuville tiukat raamit ja leluja kielletään. Verkkosivu. Viitattu 11.4.2025. https://yle.fi/a/74-20064222

Reivo, J. 2025. Tekoäly hallintaan standardeilla, standardit hallintaan tekoälyllä. Verkkosivu. Viitattu 24.4.2025. https://sfs.fi/blogi/tekoaly-hallintaan-standardeilla-standardit-hallintaan-tekoalylla/

Euroopan komissio. 2024. Harmonised Standards for the European AI Act. Verkkosivu. Viitattu 24.4.2025. https://publications.jrc.ec.europa.eu/repository/handle/JRC139430

Brewer S. 2023. Uusi ISO/IEC 42001 -standardi lisää luottamusta tekoälyyn. Verkkosivu. Viitattu 24.4.2025. https://www.dnv.fi/news/the-new-iso-iec-42001-standard-released-will-increase-trust-in-ai-250978/

CEN-CENELEC. n.d. Artificial Intelligence. Verkkosivu. Viitattu 24.4.2025. https://www.cencenelec.eu/areas-of-work/cen-cenelec-topics/artificial-intelligence/

CEN-CENELEC. 2024. INCLUSIVENESS as a common objective in AI standardization. Verkkosivu. Viitattu 24.4.2025. https://www.cencenelec.eu/news-and-events/news/2024/brief-news/2024-07-26-inclusiveness-in-ai-standardization/

Krepki R. 2024. ISO/IEC 42001 and the EU AI Act: A Compliance Guide. Verkkosivu. Viitattu 25.4.2025. https://msecb.com/iso-iec-42001-and-eu-ai-act-compliance/