

EU:N TEKOÄLYASETUS TULI VOIMAAN - raamit tekoälyn käyttöön ja kehittämiseen

Paljon keskustelua herättänyt [EU:n tekoälyasetus](#) tuli voimaan elokuun 2024 alussa. EU:n asetukset ovat suoraan jäsenvaltioissa sovellettavaa lainsäädäntöä. Myös [kansallinen toimeenpano on käynnistynyt](#) työ- ja elinkeinoministeriön johdolla.

EU:n tekoälyasetuksella annetaan Euroopan unionin alueelle yhteinen oikeudellinen kehys tekoälyjärjestelmien kehittämiseksi, markkinoille saattamiselle, käyttöönotolle ja käytölle. Soveltamisalan ulkopuolelle jäävät muun muassa yksityinen käyttö, sotilaskäyttö sekä yksinomaan tieteellistä tutkimusta ja kehittämistoimintaa varten kehitetyt tekoälyjärjestelmät ja -mallit. Tilanne on kuitenkin toinen, jos järjestelmiä tuodaan markkinoille.

Mikä on tekoälyjärjestelmä?

Tekoälyjärjestelmällä tarkoitetaan konepohjaisia järjestelmiä, jotka on suunniteltu toimimaan käyttöönoton jälkeen erilaisilla autonomian tasoilla. Järjestelmillä on siis jonkinlaista päätelykykyä. Päätelykyvyn taustalla ovat muun muassa koneoppimisen menetelmät, jotka oppivat tai joita opetetaan datan avulla. Tekoälyjärjestelmän päätelykyky on laajempi kuin perustietojenkäsittelyssä, joten tekoälyjärjestelmä voi oppia, tehdä johtopäätöksiä ja mallintaa. Asetuksessa annettu teko-

älyjärjestelmän määritelmä elää yhdessä [OECD:n tekoälymääritelmän kanssa](#).

Asetuksessa tekoälyjärjestelmät on luokiteltu riskiperustaisesti edeten minimaalisen riskin järjestelmistä kiellettyihin järjestelmiin. Kiellettyjä tekoälyjärjestelmiä ovat muun muassa ihmisten itsensä tietämättä päätöksen tekoa ja käyttäytymistä manipuloivat järjestelmät. Suuririskisinä tekoälyjärjestelminä nähdään muun muassa oppimistulosten arviointiin ja oppilaitokseen pääsemiseen liittyvät järjestelmät, koska niillä voi olla vaikutusta ihmisten tulevan toimeentulon turvaamiseen. Suuririskisiksi järjestelmiksi luokitellaan myös työsuhteen arviointiin ja uralla etenemiseen lukeutuva tekoälyjärjestelmät. Työnantajan on ilmoitettava tällaisen järjestelmän käytöstä. Suuririskisten järjestelmien käyttö ei ole kiellettyä, mutta niiden on täytettävä paljon vaatimuksia.

Rajallisia riskejä sisältäviä järjestelmiä ovat muun muassa chatbotit. Vähäisiä tai minimaalisia riskejä sisältävät yleiskäyttöiset tekoälyjärjestelmät, joista tunnetuin esimerkki on ChatGPT.

Keskeinen piirre erilaisten palveluiden ja järjestelmien arvioinnissa on läpinäkyvyys. Esimerkiksi käyttäjille on annettava tarvittava dokumentaatio järjestelmästä, tarjottava kooste käytetyistä koulutusaineistoista sekä järjestelmän tekijänoikeuslinjaus pitää olla tiedossa. Synteettistä sisältöä (kuten syväväärennöksiä) luovien tekoälyjärjestelmien on merkittävä tuotoksensa keinotekoisesti tuotetuiksi.

Tekoälylukutaito ja eettisyys

Tekoälynjärjestelmien tarjoajilla, käyttöönottajilla ja henkilöillä, joihin tekoälyjärjestelmien vaikutukset kohdistuvat, olisi oltava riittävä tekoälylukutaito. Tämä tarkoittaa osaamista ja ymmärrystä AI-järjestelmien käytön hyödyistä, riskeistä ja mahdollisista vahingoista. Komission ja jäsenvaltioiden olisi yhteistyössä sidosryhmien kanssa edistettävä tekoälylukutaitoa esimerkiksi laatimalla käytännesääntöjä tekoälyä kehittäville sekä niiden toiminnasta ja käytöstä vastaaville tahoille.

Tieteellisissä kirjastoissa tekoälylukutaidon käsite yhdistetään tuttuun informaatiolukutaidon käsitteeseen, mikä liittyy käytännössä tiedonhankinnan ja tiedonhallinnan opetukseen. Tekoälylukutaitoon liittyy myös algoritmien ja rajapintojen luomisen taso, mikä on taas lähempänä järjestelmiä ja datanhallintaa. Tekoälylukutaitoa koskevat kohdat asetuksesta tulevat sovellettavaksi jo vuoden 2025 alkupuolella, joten monissa korkeakouluissa on

mahdollisesti jo aloitettu valmistelut opiskelijoiden ja henkilöstön riittävän tekoälylukutaidon varmistamiseksi.

Komission nimittämä korkea tason tekoälytyöryhmä laati [luotettavaa tekoälyä koskevat eettiset ohjeet](#) vuonna 2019. Seitsemän periaatetta tekoälyjärjestelmälle ovat ihmisen toimijuus ja ihmisen suorittama valvonta, tekninen vakaus ja turvallisuus, yksityisyyden suoja ja datanhallinta, avoimuus, monimuotoisuus, syrjimättömyys ja oikeudenmukaisuus sekä yhteiskunnallinen ja ympäristöön liittyvä hyvinvointi ja vastuuvollisuus. Avoimuus tarkoittaa järjestelmien kehittämisen ja käytön jäljitettävyyttä ja selitettävyyttä. Ihmisten tulisi myös olla tietoisia, milloin he viestivät ja ovat vuorovaikutuksessa tekoälyjärjestelmän kanssa. Asetuksessa kannustetaan ottamaan nämä vaatimukset huomioon, kun kehitetään parhaita käytäntöjä ja standardeja. Tekoälyn eettistä arviointia varten on muun muassa [Unescon laatima opas](#), johon voi tukeutua järjestelmiin tustuesssa.

Suuria kysymyksiä, vähän vastauksia

Tekoälyasetus ei synny tyhjiöön. Palveluiden kehittämiseen ja laillisuuden arviointiin vaikuttaa myös jo olemassa oleva lainsäädäntö, kuten kansallisella tasolla tekijänoikeuslaki

Ihmisten tulisi myös olla tietoisia, milloin he viestivät ja ovat vuorovaikutuksessa tekoälyjärjestelmän kanssa.

ja digipalvelulaki. Yhtymäkohtia yleiseen tietosuoja-asetukseen on paljon, mutta tekoäly-asetuksessa korostetaan näiden säädösten erillisyyttä.

Komissiolla on jatkossa oma [tekoälytoimisto](#), jonka tehtävänä on luoda käytännesääntöjä tekoälyn käytölle ja valvoa niiden toteutumista. Komissiota puolestaan tukee Euroopan tekoälyneuvosto, joka kokoaa yhteen jäsenvaltioiden korkean tason edustajat.

Suuria kysymyksiä leijuu ilmassa, mutta valmiita vastauksia on vielä vä-

hän. Korkeakoulusektorin ohjeistuksessa ja yleisessä keskustelussa hypetys lienee jo vähenemässä, ja riskinäkökulmaa tulee luonnollisesti enemmän mukaan tekoälyasetuksen soveltamisen edetessä. Käytännönläheisempiä artikkeleita tekoälysäätelyn vaikutuksista tullaan varmasti näkemään myös Signumissa. Kannattaa seurata korkeakoulutuksen ja tutkimuksen digitalisoitumisen tiekarttaa [ka.csc.fi](#), jossa tekoälylle on oma osionsa ja paljon lisätietoa. ♦

Kirjoittaja

SOILE MANNINEN

Helsingin yliopiston kirjasto

soile.manninen@helsinki.fi

<https://orcid.org/0000-0003-1009-1180>



Tekoälyasetuksen soveltamisen eteneminen

