VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

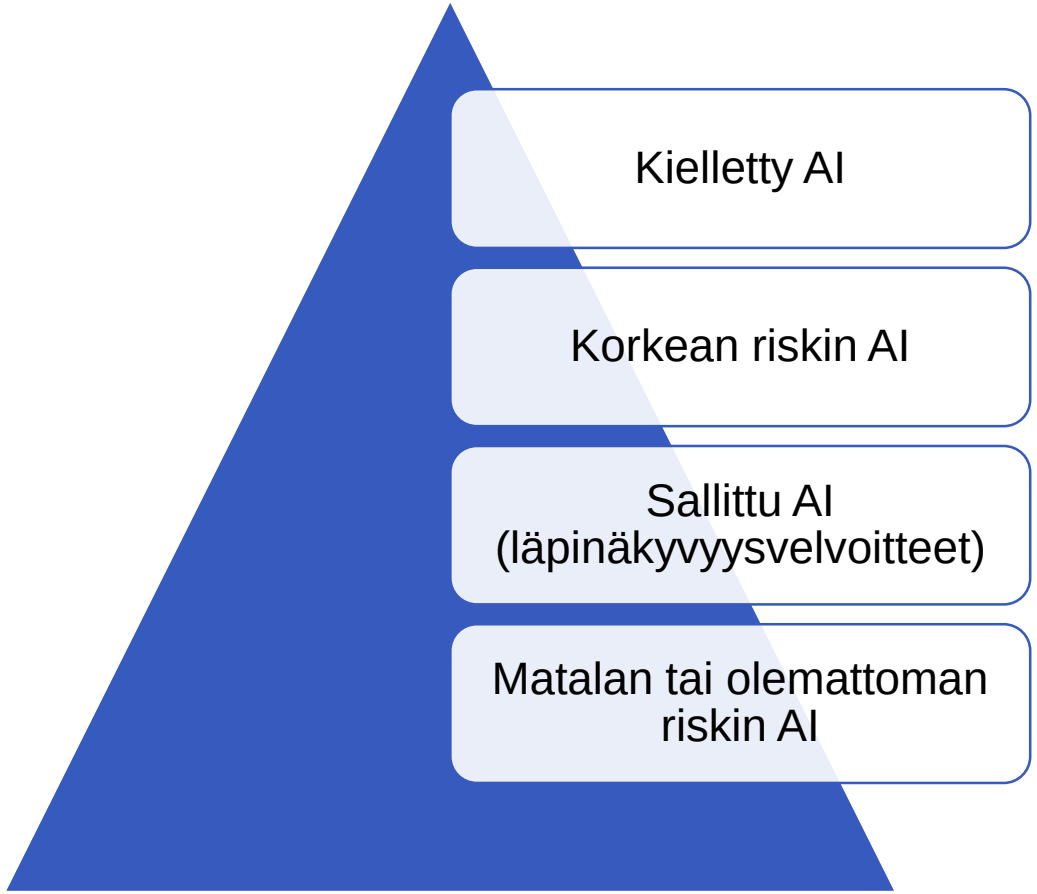
EU-sääntely tietojärjestelmäsääntelyn kehittämisvaatimuksina

Maria Kekäläinen, neuvotteleva virkamies
4.5.2021
Julkisen hallinnon tietojärjestelmiä koskevan yleislainsäädännön tarkistamista valmistelevan työryhmän kokous

AI-säädösehdotuksen keskeinen sisältö

- Koskee tekoälyjärjestelmien käyttöä ja markkinoille laskemista.
- Tietyt tekoälyn käyttötarkoitukset kielletään kokonaan.
- Ns. korkean riskin tekoälyjärjestelmiin kohdistuu erityisiä vaatimuksia.
- Tiettyjä tekoälyn käyttötarkoituksia koskevat erityiset läpinäkyvyysvaatimukset.
- Asetusta sovelletaan unionissa sijaitseviin tekoälyjärjestelmiin sekä tekoälyjärjestelmien maahantuojiin, kehittäjiin ja käyttäjiin.

Riskiperustainen sääntely



Tekoälyjärjestelmän määritelmä (artikla 3(1) ja liite I)

‘artificial intelligence system’ (AI system) means software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

Liite I, jota voidaan muuttaa delegoidulla asetuksella:

(a) Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

(b) Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems; ➡ Koskisi mahd. tietojärjestelmiä julkisella sektorilla

(c) Statistical approaches, Bayesian estimation, search and optimization methods

Kielletyt tekoälyn käyttötarkoitukset (artikla 5)

- Alitajuisesti (subliminal) henkilön käytökseen vaikuttaminen haitallisesti tai tavalla joka on omiaan aiheuttamaan haittaa.
- Haavoittuvassa asemassa olevien ihmisryhmien hyväksikäyttäminen tavalla joka aiheuttaa tai on omiaan aiheuttamaan haittaa.
- Henkilöiden luotettavuuden tai käytöksen pisteyttäminen (social scoring) julkisen hallinnon toimesta, jos pisteyttämistä käytetään ihmisten tai ihmisryhmien eriarvoiseen kohtelemiseen ja tietoja käytetään irrallaan alkuperäisestä asiayhteydestään.
- Reaaliaikainen etänä tapahtuva biometrinen tunnistaminen ilman painavaa, lueteltua syytä; jos käytetään, käyttöön kohdistuu erilaisia rajoituksia.

Korkean riskin tekoälyjärjestelmät (Artiklat 6-51)

- Tekoälyjärjestelmät, joita käytetään laitteiden turvallisuuskomponenttina sektoreilla, joita säädellään liitteessä II mainituilla EU-säädöksillä, mm.:
  - Koneet (machinery)
  - Lelut
  - Radiolaitteet
  - Lääkinnälliset laitteet ja koneet
  - Suojavarusteet
- Tekoälyjärjestelmät, joita käytetään liitteen III mainitsemissa tarkoituksissa, mm.:
  - Etänä tapahtuva biometrinen tunnistaminen (ei vain reaaliaikainen)
  - Kriittisen infrastruktuurin ylläpito ja hallinta
  - Koulutukseen sisään ottaminen ja opintosuoritusten arviointi
  - Työhön ottaminen ja irtisanominen
  - Pääsy/käyttö julkisiin palveluihin ja etuuksiin sekä keskeisimpiin yksityisiin palveluihin
  - Luottokelpoisuus
  - Lainvalvonta ja –käyttö
  - Maahanmuutto

Korkean riskin tekoälyjärjestelmiin kohdistuvat vaatimukset (artiklat 9-15)

- Riskinhallintajärjestelmä
- Lokijärjestelmä
- Ihminen valvoo ja minimoi aiheutuvat riskit ja haitat; ihmisen on ymmärrettävä, mitä järjestelmä tekee, ja hänen on voitava pysäyttää järjestelmä tai puuttua sen toimintaan
- Tarkka (accurate)
- Vikasietokykyinen
- Kyberturvallinen
- Datanhallintajärjestelmä (data governance)
- Riittävä tekninen dokumentaatio
- Riittävän läpinäkyvä käyttäjälle; selkeät ja kattavat käyttöohjeet

Korkean riskin AI-järjestelmät – toimijoiden velvoitteet

Provider obligations

- Establish and Implement **quality management** system in its organisation
- Draw-up and keep up to date **technical documentation**
- **Logging** obligations to enable users to monitor the operation of the high-risk AI system
- Undergo **conformity assessment** and potentially re-assessment of the system (in case of significant modifications)
- Register AI system in EU database
- Affix CE marking and sign declaration of conformity
- Conduct **post-market monitoring**
- **Collaborate** with market surveillance authorities

User obligations

- Operate AI system in accordance with **instructions of use**
- Ensure **human oversight** when using of AI system
- **Monitor** operation for possible risks
- **Inform the provider or distributor about any serious incident** or any malfunctioning
- **Existing legal obligations** continue to apply (e.g. under GDPR)

Korkean riskin tekoälyjärjestelmien valvonta (artiklat 30-51)

- Tekoälyjärjestelmän vaatimuksenmukaisuus varmistetaan joko sisäisellä tai ulkoisella tarkastuksella. Tarkastustapa riippuu siitä, mistä liitteen III mukaisesta käyttötarkoituksesta on kyse.
  - Jos kyse on turvakomponentista laitteessa, josta säädetään liitteessä II mainitulla sääntelyllä, tarkastus tehdään ao. sääntelyn mukaisella menettelyllä.
- Sisäisessä tarkastuksessa tutkittavat seikat on kuvattu tarkemmin liitteessä VI ja ulkoisessa tarkastuksessa tutkittavat liitteessä VII.
- Tarkastus on uusittava järjestelmän muuttuessa olennaisesti.
- Jäsenvaltioiden nimeämät viranomaiset voivat määritellä **ilmoitettuja laitoksia (notified bodies)**. Nämä tarkistavat, että korkean riskin tekoälyjärjestelmä vastaa asetuksessa säädettyjä vaatimuksia.

Jälkivalvonta (artiklat 61-62)

- Korkean tekoälyjärjestelmän toimittajan on huolehdittava riittävästä jälkivalvonnasta, kun järjestelmä on otettu käyttöön.
- Jälkivalvonnasta on laadittava suunnitelma.
- Vakavista vika- ja virhetilanteista on ilmoitettava valvontaviranomaisille.

Tiettyjä tekoälyjärjestelmiä koskeva läpinäkyvyys (artikla 52)

- Ihmisten kanssa toimivien järjestelmien on kerrottava ihmiselle, että kyseessä on tekoälyjärjestelmä, tai ne on suunniteltava niin, että ihminen ymmärtää tämän, ellei se muuten ole ilmeistä.
- Tunteita tunnistavien ja biometrisiä tietoja luokitteluun käyttävien järjestelmien käyttäjien on kerrottava ihmiselle, johon niitä käytetään, että heihin käytetään ao. järjestelmää.
- Tekoälyllä luodun aitoa muistuttavan kuva- tai äänisisällön yhteydessä on kerrottava, että kyse tekoälyllä luodusta sisällöstä (ns. deep fake).
- Mitä edellä on mainittu ei sovelleta, jos tarkoituksena on rikosten paljastaminen, estäminen tai selvittäminen.

Asetusehdotuksen jatkokäsittely

- **Kansallinen käsittely**
  - U-kirjeen ja Suomen kannan muodostus toukokuussa 2021
  - U-kirje EU-jaostojen käsittelyssä 7. – 11.5.2021
- **EU-tason käsittely**
  - EU:n neuvosto ja europarlamentti käsittelevät asetusehdotusta ja tekevät siihen muutosehdotuksensa
  - Neuvostossa käsittely aloitetaan Portugalin EU-pj-kaudella 2021
  - Käsittely jatkuu Slovenian EU-pj-kaudella 2021

Vaikutukset kansalliseen tietojärjestelmäsääntelyyn (1/2)

- AI:n määritelmä kattaa mahdollisesti tietojärjestelmät julkisella sektorilla
- Korkean riskin AI-järjestelmät kattaa julkisella sektorilla käytettäviä järjestelmiä
  - Koskee sekä hallintopäätösten tekemistä että tosiasiallista hallintotoimintaa
  - Esim. pääsy julkisiin palveluihin ja etuuksiin, oikeuslaitoksessa tehtävä tosiasioiden selvittäminen, matkustusasiakirjojen aitouden selvittäminen
- Asetuksen mahdollinen päällekkäisyys kansallisen sääntelyn kanssa
  - Vaatimuksia mm. tietoaineistojen laadulle, toimintavarmuudelle ja läpinäkyvyydelle
  - Suomessa viranomaistoimintaa koskee jo esim. tiedonhallintasääntely ja hyvän hallinnon periaatteet – lieventää asetuksen vaikutuksia viranomaistoimintaan

Vaikutukset kansalliseen tietojärjestelmäsääntelyyn (2/2)

- Epävarmaa, kuinka sääntely vaikuttaa viranomaisen neuvontapalveluissa käytössä oleviin keskusteluro botteihin (chatbotit)
  - Chatbotit voivat hyödyntää liitteen I tekoälyteknologiaa ja kuulua liitteen III korkean riskin kategoriaan
- Julkisen sektorin toimija – AI järjestelmän ”toimittajan” vai ”käyttäjän roolissa”?
  - Toimittajaa ja käyttäjää koskevat erilaiset velvollisuudet asetuksessa

EU:n kyberaloitteet

NIS- ja CER-direktiivit

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

NIS 2.0 –direktiivi (tieto- ja verkkoturvadirektiivi)

- Komission direktiiviehdotus joulukuussa 2020
- Tavoitteena on vahvistaa kyberturvallisuuden tasoa kriittisiksi katsottujen sektoreiden ja toimijoiden osalta asettamalla riskienhallintatoimia, mm.:
  - Riskianalyysit ja tietojärjestelmien turvallisuustoimet
  - Häiriöiden käsittely (ennaltaehkäisy, tunnistaminen ja häiriöihin vastaaminen)
  - Liiketoiminnan jatkuvuus ja kriisinhallinta
  - Tuotantoketjujen kyberturvallisuus
  - Haavoittuvuuksien käsittely ja tunnistaminen

NIS 2.0 –direktiivi (tieto- ja verkkoturvadirektiivi)

- NIS 2.0 soveltamisalan laajennetaan koskemaan mm. julkishallinnon toimijoita
  - Mm. keskushallinnon toimijat sekä alueelliset hallinnot sellaisina kuin ne on määritelty asetuksessa (EU) 1059/2003
  - Ei koske julkishallintoa yleisen turvallisuuden, lainvalvonnan, puolustuksen ja kansallisen turvallisuuden aloilla
- NIS 1.0 implementoitiin kansallisesti sektorikohtaiseen sääntelyyn, mm. L sähköisen viestinnänpalveluista, IlmailuL, RautatieL
- NIS 2.0 kansallisessa täytäntöönpanossa julkishallintoa koskevaa lainsäädäntöä tulisi tarkastella

CER-direktiivi (kriittisten toimijoiden häiriönsietokyky)

- Tavoitteena parantaa välttämättömien palvelujen tarjontaa toimilla, jotka ylläpitävät ja parantavat kriittisten toimijoiden häiriönsietokykyä
- CER korvaa Euroopan kriittisen infrastruktuurin suojaamista koskevan ECI-direktiivin (2008)
- Linjassa NIS 2.0-direktiiviehdotuksen kanssa
- CER-direktiiviehdotus koskee kymmentä eri sektoria, kuten julkista hallintoa

CER-direktiivi (kriittisten toimijoiden häiriönsietokyky)

- Direktiivillä tavoitellaan keinovalikoiman laajentamista pelkistä suojaustoimista elintärkeiden toimintojen jatkuvuudenhallintaa kehittäviin toimiin
- Direktiivi määrittää kansalliset toimenpiteet kriittisten toimijoiden häiriönsietokyvyn parantamiseksi, mm.:
  - Toimivaltaisten viranomaisten on laadittava luettelo olennaisista palveluista ja suoritettava säännöllisesti kaikkien asiaankuuluvien riskien arviointi
  - Kriittisten toimijoiden on säännöllisesti arvioitava tunnistetut ja merkittävät riskit toimialallaan
  - Järjestelyt, joilla varmistetaan, että kriittiset toimijat ilmoittavat viipymättä toimivaltaiselle viranomaiselle merkittävistä häiriötilanteista