Amnesty International Suomen osasto

Lausunto

04.12.2024

Asia: VN/17593/2024

Lausuntopyyntö: luonnos hallituksen esitykseksi tekoälyasetuksen toimeenpanoa koskevaksi lainsäädännöksi

Lausunnonantajan lausunto

Lausuntonne koskien keskeisiä ehdotuksia

-

Lausuntonne koskien vaikutusten arviointia

-

Lausuntonne koskien säännöskohtaisia perusteluita

-

Lausuntonne koskien pykäliä

-

Muut kommentit HE -luonnoksesta

1. Yleistä

Tekoälyasetuksen (EU 2024/1689) tarkoituksena on varmistaa, että markkinoille tuotavat tai käyttöönotettavat tekoälyjärjestelmät eivät vaaranna ihmisten turvallisuutta, terveyttä tai perusoikeuksia.

Asetus on astunut voimaan 1.8.2024 ja sen soveltaminen alkaa vaiheittain. Hallituksen esitysluonnoksessa ehdotetaan säädettäväksi uusi laki eräiden tekoälyjärjestelmien valvonnasta, jossa nimettäisiin toimivaltaiset markkinavalvontaviranomaiset ja ilmoittamisesta vastaavat viranomaiset. Eräiden tuotteiden markkinavalvonnasta annetun lain (1137/2016) soveltamisalaa laajennettaisiin siten, että siihen lisättäisiin laki eräiden tekoälyjärjestelmien valvonnasta ja lakiin lisättäisiin asetuksen nojalla nimetyt viranomaiset toimivaltaisiksi markkinavalvontaviranomaisiksi.

Amnesty International katsoo, että vaikka tekoälyasetus on huomattava askel tekoälyn sääntelyssä, se ei suojaa ihmisoikeuksia tarvittavalla tavalla (kts. https://www.amnesty.org/en/latest/news/2024/03/eu-artificial-intelligence-rulebook-fails-to-stop-proliferation-of-abusive-technologies/). Asetukseen jäi vakavia puutteita ihmisoikeuksien suojelun kannalta. Se ei sisällä riittäviä säännöksiä vastuuvelvollisuudesta tai läpinäkyvyydestä. Se ei myöskään kiellä haitallisen valvontateknologian vientiä EU:n ulkopuolelle.

Tekoälyn riskiperusteisen sääntelyn vaikuttavuus perustuu riskien tehokkaaseen ennakolliseen tunnistamiseen ja luokitteluun. Riskien realisoitumisen ehkäisemiseksi kansallisella tasolla on välttämätöntä, että asetuksen toimeenpanossa kiinnitetään huomiota säädökseen sisältyviin riskien tunnistamiseen liittyviin aukkoihin ja sääntelyn jälkivalvontaan. Kaupalliset ja kilpailulliset intressit eivät saa tulla perus- ja ihmisoikeuksien turvaamisen edelle asetuksen kansallisessa täytäntöönpanossa.

2. Tekoälyjärjestelmien käyttöön liittyy aina laajamittaisia uhkia perus- ja ihmisoikeuksille

Tekoälyjärjestelmien käytön merkittävimmät perus- ja ihmisoikeuksiin kohdistuvat riskit koskevat niiden potentiaalia toisintaa syrjiviä asenteita laajassa mittakaavassa. YK:n entinen rasismin nykyaikaisten muotojen erityisraportoija E. Tendayi Achiume on todennut, että algoritmien käytön merkittävänä haasteena on se, että ne ”toistavat laajamittaisiin tietokokonaisuuksiin sisältyviä ennakkoluuloja, jotka kykenevät jäljittelemään ja toisintamaan ihmisten implisiittisiä ennakkoluuloja” (A/HRC/44/57, k. 7).

Hallituksen esitysluonnoksessa on perus- ja ihmisoikeusvaikutusten osalta tuotu esiin, että suuririskisten tekoälyjärjestelmien valvonnalla voitaisiin torjua tekoälyjärjestelmän käyttämän datan myötä aiheutuvista vinoumista syntyviä haittoja, minkä vuoksi valvonta edistäisi myös henkilöiden yhdenvertaisuuden toteutumista (HE s. 94). Perus- ja ihmisoikeusvaikutusten arviointi esitysluonnoksessa lähtee kuitenkin pitkälti siitä, että valvonta ja sääntely on riittävää torjumaan tekoälyjärjestelmien aiheuttamat ihmisoikeusriskit. Arvioinnissa voisi tuoda esille myös mahdolliset riskit perus- ja ihmisoikeuksien kannalta, mikäli valvonta ei ole riittävää ja miten riskejä aiotaan torjua.

Samalla esitetty kansallinen sääntely edustaa lievintä asetuksen sallimaa suuririskisten tekoälyjärjestelmien rajoituslinjaa, joka käytännössä mahdollistaa useita perus- ja ihmisoikeuksien toteutumisen kannalta riskialttiita tekoälyjärjestelmien käyttötapoja muun muassa viranomaistoiminnassa.

3. Reaaliaikaisten biometristen etätunnistusjärjestelmien kiellon poikkeukset mahdollistavat väärinkäytön

Asetus jättää jäsenvaltioille melko paljon liikkumavaraa sen suhteen, miten tiukan kiellon ne asettavat kansallisessa lainsäädännössään esimerkiksi reaaliaikaisten biometristen etätunnistusjärjestelmien käyttöön julkisilla paikoilla (ks. 5 art. 5 k. ja HE s. 38). Reaaliaikaisella biometrisellä etätunnistusjärjestelmällä tarkoitetaan biometristä etätunnistusjärjestelmää, jossa biometristen tietojen kerääminen, vertailu ja tunnistaminen tapahtuvat ilman merkittävää viivettä ja joka kattaa välittömän tunnistamisen lisäksi myös vähäiset viiveet, joilla pyritään ehkäisemään harhaanjohtamista (3 art. 42 k.). Reaaliaikaisten biometristen etätunnistusjärjestelmien käyttö on asetuksen 5 artiklan 1 kohdan h alakohdan nojalla lähtökohtaisesti kiellettyä lainvalvontatarkoituksessa julkisissa tiloissa, mutta niiden käyttö voidaan sallia myös lainvalvontatarkoituksessa 5 artiklan d kohdan i-iii alakohtien mukaisissa erityistilanteissa.

Biometristen tunnistusjärjestelmien käytöllä on vakavia seurauksia muun muassa kokoontumisvapauden, sananvapauden, yhdenvertaisuuden ja yksityisyydensuojan toteutumiseen. Amnesty International ja yli 170 muuta organisaatiota laativat vuonna 2021 avoimen kirjeen, jossa järjestöt vaativat kasvojentunnistus- ja biometristen etätunnistustekniikoiden käytön kieltämistä niiden ihmisoikeuksia vakavasti uhkaavan luonteen takia. Kirjeessä järjestöt toteavat, että biometriset tunnistusjärjestelmät mahdollistavat massavalvonnan ja syrjivän kohdennetun valvonnan, minkä lisäksi valvontainfrastruktuurin luominen ja ylläpitäminen poikkeustilanteita varten avaa oven väärinkäytöksille (ks. https://www.amnesty.org/en/latest/press-release/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/).

Perustuslakivaliokunta on komission alkuperäisen asetusehdotuksen suhteen kuitenkin katsonut, että biometrisen etätunnistuksen kiellosta tehtävien poikkeusten perusteluja voidaan lainvalvonnan kannalta pitää sinänsä varsin painavina, kun lisäksi otetaan huomioon, että etätunnistuksen tarkoituksena on myös suojata henkilökohtaista turvallisuutta ja sitä tukevan lainvalvonnan edellytyksiä (PeVL 37/2021 vp, s. 10). Tilanteissa, joissa järjestelmän käyttöönotto on poikkeuksen nojalla mahdollista lainvalvontatarkoituksessa, ja viranomaisella on asiassa harkintavaltaa, korostuu viranomaisen velvollisuus perus- ja ihmisoikeusmyönteiseen päätöksentekoon.

Asetuksen kansallisessa täytäntöönpanossa on painavana seikkana huomioitava, että reaaliaikaisten biometristen etätunnistusjärjestelmien vakavien väärinkäytösten riski on läsnä aina, kun ne ovat lainsäädäntöön tehdyin poikkeusperustein viranomaisten käytettävissä, ja kun yksityisen sektorin toimijoilla on kaupallinen intressi jatkaa niiden kehittämistä. Järjestelmien kieltoon tehtyjen poikkeusten nojalla tapahtuvan käytön valvonnan tulee olla systemaattista, läpinäkyvää ja tehokasta, mikä vaatii riittävien taloudellisten resurssien kohdentamista valvontatoimenpiteisiin ja valmiutta muuttaa lainsäädäntöä matalalla kynnyksellä, mikäli väärinkäytöksiä ja uhkia perus- ja ihmisoikeuksien toteutumiselle ilmenee. Erityistä painoarvoa on annettava lisäksi järjestelmien käytöstä tehtävän raportoinnin läpinäkyvyydelle: kansallisten markkinavalvontaviranomaisten ja jäsenvaltioiden kansallisten tietosuojaviranomaisten on 5 artiklan 6 kohdan mukaan toimitettava

komissiolle vuosittain raportti biometristen etätunnistusjärjestelmien käytöstä julkisissa tiloissa lainvalvontatarkoituksiin (ks. HE s. 16).

Maahanmuuttoon liittyvä tekoälyn käyttö on yksi esimerkki erityisen riskialttiista käyttöalasta. Tekoälyä käytetään maahanmuuton hallinnassa yhä enemmän. Muun muassa biometriset luokittelujärjestelmät ja kasvojentunnistustietokannat sekä profilointi sisältävät väärinkäytösten riskejä, vaikka niiden käyttöön liittyisikin suojatoimia. Niiden käyttö maahanmuuttojärjestelmissä ylipäänsä on arveluttavaa, mutta niihin liittyy riski myös arkaluontoisten tietojen päätymisestä vääriin tarkoituksiin.

Esimerkiksi automatisoituja riskinarviointi- ja profilointijärjestelmiä ei tulisi käyttää sen määrittelemiseksi liittyykö siirtolaisiin ja turvapaikanhakijoihin mahdollisesti turvallisuusuhan riskiä. Näihin järjestelmiin liittyy suuri syrjinnän, yksityisyyden- ja tietosuojan loukkauksen sekä vapauden ja turvallisuuden loukkauksen riski. Myös siirtolaisten ja turvapaikanhakijoiden liikkeitä ennustavat järjestelmät aiheuttavat ihmisoikeusloukkausten riskejä, sillä niitä käytetään herkästi maahanmuuton ja turvapaikanhaun estämiseen sekä rajoittamiseen, mikä saattaa loukata palautuskieltoa tai estää turvapaikanhakuoikeuden toteutumista.

Tekoälyyn pohjautuvat petostarkoitusta havaitsevat ja muut tunteita havaitsevat järjestelmät muodostavat myös ihmisoikeusloukkausten riskin eikä niitä tule käyttää esimerkiksi turvapaikkamenettelyssä. Kyseisenlaiset järjestelmät saattavat muodostaa riskin syrjinnälle sekä yksityisyydensuojan ja oikeudenmukaisen oikeudenkäynnin loukkauksille.

Sekä jälkikäteiset että reaaliaikaiset biometriset tunnistus- ja luokittelujärjestelmät ylipäänsä mahdollistavat massavalvonnan sekä valvonnan syrjivän luonteen, mikä siirtolaisuuden ja turvapaikanhaun kontekstissa vaarantaa palautuskiellon periaatteen toteutumista. Rajavartiolaitoksen toimivaltuudet ovat rajavalvonnassa jo tällä hetkellä hyvin laajat teknisten järjestelmien käytössä eikä tämän mahdollisia ihmisoikeusloukkausten riskejä ole aiemmissakaan lakimuutoksissa arvioitu. Myös lainvalvontatarkoituksissa mahdollinen biometristen tunnisteiden reaaliaikainen käyttö voi tulevaisuudessa johtaa laajentuvaan käyttöalaan, myös siirtolaisuuteen nähden.

Järjestelmien käytössä ja niiden valvonnassa tulee huomioida maahanmuuton ja turvapaikanhaun näkökulmasta olennaiset ihmisoikeusloukkausten riskit myös tulevaisuuden käyttötapoja arvioitaessa. Siksi ihmisoikeusvaikutusten arviointi ja –loukkausten riskin tiedostaminen sekä sääntelyn läpinäkyvyys ovat avainasemassa tekoälyn käyttöön liittyvien ihmisoikeusloukkausten estämisessä.

4. Sosiaalisen pisteytyksen järjestelmien kielto ei estä kaikkea algoritmien syrjivää käyttöä viranomaistoiminnassa

Sosiaaliseen pisteytykseen käytettävät tekoälyjärjestelmät ovat asetuksen nojalla lähtökohtaisesti kiellettyjä silloin, kun niiden käyttö johtaa syrjintään. Tekoälyjärjestelmien markkinoille saattaminen, käyttöönotto tai käyttö luonnollisten henkilöiden tai henkilöryhmien arvioimiseksi tai luokittelemiseksi heidän sosiaalisen käyttäytymisensä tai tunnettujen, pääteltyjen tai ennakoitujen henkilökohtaisten ominaisuuksiensa tai luonteenpiirteidensä perusteella on kiellettyä silloin, kun sosiaalinen pisteytys johtaa tiettyjen luonnollisten henkilöiden tai henkilöryhmien haitalliseen tai epäedulliseen kohteluun sosiaalisissa yhteyksissä, jotka eivät liity siihen asiayhteyteen, jossa tiedot alun perin tuotettiin tai kerättiin, tai tiettyjen luonnollisten henkilöiden tai henkilöryhmien haitalliseen tai epäedulliseen kohteluun, joka on perusteetonta tai suhteetonta heidän sosiaaliseen käyttäytymiseensä tai sen vakavuuteen nähden (5 art. 1 k. c alak. i-ii alak.).

Syrjivän sosiaalisen pisteytyksen kiellosta huolimatta asetus mahdollistaa tekoälyjärjestelmien käytön lukuisissa riskialttiissa tarkoituksissa, kuten sosiaaliturvaetuuksien hakemusten käsittelyssä.

YK:n äärimmäisen köyhyyden ja ihmisoikeuksien erityisraportoija on todennut, että esimerkiksi sosiaaliturvan riskien pisteyttämiseen ja tarpeiden luokitteluun käytettävät uudet teknologiat vaikuttavat myös moniin muihin hyvinvointivaltion aloihin, ja että yksilön oikeuksien määrittelyyn yleisen väestöryhmän käyttäytymisestä johdettujen ennusteiden perusteella liittyy useita ongelmia (A/74/493, k. 28).

Amnesty on julkaissut runsaasti tutkimuksia algoritmien käytöstä sosiaaliturvan hallinnoinnissa, esimerkiksi mahdollisten väärinkäytösten havaitsemiseksi. Tutkimukset koskevat muun muassa Serbiaa, Alankomaita, Intiaa, Ruotsia ja Tanskaa. Lisäksi Amnesty on mukana Ranskan korkeimpaan hallinto-oikeuteen jätetyssä valituksessa, joka koskee tekoälyn käyttöä sosiaaliturvan hallinnoinnissa.

Marraskuussa 2024 Amnesty International julkaisi raportin petostentorjunta-algoritmien käytöstä Tanskan sosiaaliturvaviranomaisen Udbetaling Danmarkin (UDK) sekä valtion mandaatilla toimivan yrityksen Arbejdsmarkedets Tillægspension (ATP) etuuskäsittelytoiminnassa (Amnesty International: Coded Injustice: Surveillance and Discrimination in Denmark’s automated welfare state, julkaistu 12.11.2024. Saatavilla: https://www.amnesty.org/en/documents/eur18/8709/2024/en/). Raportin mukaan UDK:n, ATP:n ja kuntien käytännöt ovat luoneet valvontajärjestelmän, joka loukkaa yksilöiden ihmisarvoa sekä oikeutta yksityisyyteen, minkä lisäksi etuusjärjestelmä luo marginalisoiduille ryhmille, kuten kriisitilanteissa oleville naisille ja vammaisille henkilöille esteitä sosiaalietuuksien saamiselle, mikä voi vaarantaa kyseisten ryhmien oikeuden sosiaaliturvaan (ks. Amnesty International 2024, s. 79). Raportti osoittaa, että sosiaalisen pisteytyksen kaltaisia tekoälyjärjestelmiä käytetään EU-valtioiden viranomaistoiminnassa tälläkin hetkellä.

Asetuksen kansallisessa toimeenpanossa tulisi kieltää, että tekoälyasetuksen mahdollistamat potentiaalisesti marginalisoituja ryhmiä syrjivät tekoälyjärjestelmien käyttötavat viranomaistoiminnassa. Amnesty kyseenalaistaa tutkimuksissa ilmenneiden väärinkäytösten vuoksi

tekoälyn käytön sosiaaliturvan mahdollisten väärinkäytösten havaitsemiseksi ylipäätään. Suomessa tiedetään sosiaaliturvan alikäytön olevan väärinkäytöksiä laajempi ongelma. Ihmisoikeuksien kannalta riskialttiin teknologian käyttöönottoa tulisi harkita tarkoituksenmukaisuuden ja kohtuullisen näkökulmasta.

5. Sääntelyn vaikuttavuuden läpinäkyvään valvontaan on osoitettava riittävästi resursseja

Tekoälyjärjestelmien käytön lisääntymisestä johtuvia riskejä on vaikeaa tyhjentävästi ennustaa, minkä vuoksi tekoälyasetuksen kansallisessa toimeenpanossa tulee huomioida sääntelyn keskeneräisyys. Sääntelytarpeet tulevat lisääntymään uusien tekoälyn käyttötapojen tullessa markkinoille, eikä asetuksen myötä suoraan voimaan tullutta sekä ehdotettua kansallista sääntelyä tule nähdä lopullisena ratkaisuna tekoälyjärjestelmien käytön rajoittamiseen ja valvontaan.

Markkinavalvontaviranomaisten rooli tekoälyasetuksen täytäntöönpanon valvojina tulisi olemaan merkittävä. Valvontatehtävät on hajautettu eri markkinavalvontaviranomaisille, joilla tulisi olemaan markkinavalvontalain (1137/2016) 3 luvun mukaiset toimivaltuudet ja mahdollisuus tehostaa määräyksiään uhkasakoin. Valvonnan tehokkuus tehtävien lisääntyessä vaatii riittävien resurssien allokoimista markkinavalvontaviranomaisten valvontatehtäviin. On myös varmistettava valvontaviranomaisten riittävä osaaminen uusiin valvontatehtäviin. Myös Suomen kansallisella markkinavalvontastrategialla on merkitystä muun muassa käytössä olevien valvontaresurssien tehokkuuden ja vaikuttavuuden varmistamisessa (ks. HE s. 70). Seuraavassa markkinavalvontastrategiassa on otettava asianmukaisesti huomioon usealle viranomaiselle osoitettavat uudet toimintavastuut ja niihin liittyvät resurssitarpeet.

Kuten edellä on todettu, tekoälyasetuksen toimeenpano ei merkitse sääntelyn lopullisen tason saavuttamista. Sääntelyn aukkojen ja lisäsääntelyn tarpeen tunnistaminen vaatii paitsi taloudellisten resurssien suuntaamista markkinavalvontaan, myös läpinäkyvää vaikutusten arviointia ja panostamista julkiseen raportointiin. Tekoälyjärjestelmät tulevat koskettamaan yhä useampia elämän osa-alueita, minkä takia myös sääntelyn vaikuttavuuden jälkivalvonnan tulee koostua laaja-alaisesta yhteistyöstä eri viranomaisten ja kansalaisyhteiskunnan toimijoiden välillä. Lainsäätäjällä tulee olla myös valmius muuttaa ja kehittää lainsäädäntöä asetuksen puitteissa jälkivalvonnassa havaittujen sääntelyn aukkojen täyttämiseksi.

Esitysluonnoksessa on tuotu esiin, miksi valvontatehtävien hajauttaminen on perusteltua. Hajautettu malli aiheuttanee kuitenkin jonkinasteista päällekkäisyyttä sekä korostunutta tarvetta tiedon jakamiselle sekä koordinoinnille. Esityksen jatkovalmistelussa voisi olla syytä harkita hajautetun valvonnan tueksi valvontakokonaisuuden koordinoinnin ja raportoinnin, kokonaiskuvan hahmottamisen ja sääntelyn kehittämistarpeiden arviointia yhdelle viranomaiselle, esimerkiksi tietosuojavaltuutetulle. Tämä voisi edistää valvonnan toimivaa koordinaatiota, valvontakokonaisuuden toimivaa koordinaatiota, kehittämistarpeiden kokoamista sekä kokoavaa raportointia.

Jos organisaationne toimii tiedonhallintalain (906/2019) tarkoittamana tiedonhallintayksikkönä, mitkä ovat näkemyksenne hallituksen esityksen luonnoksen 4.2.6. kappaleeseen ”Tiedonhallinnan muutosvaikutukset” organisaationne koskevan tiedonhallinnan osalta?

-

Toimiiko organisaationne tai edustamanne yritys tekoälyasetuksen tarkoittamana toimijana, ja jos toimii, millä tavoin katsotte, että asetus ja ehdotettavat lait vaikuttavat organisaatioonne tai yritykseenne?

-

Sato Mariko
Amnesty International Suomen osasto