

07.09.2021

POL-2021-105644

Pekka Sallinen
Poliisitarkastaja

Eduskunnan lakivaliokunta

Asiantuntijalausunto komission tiedonannosta eurooppalaisesta lähestymistavasta tekoälyyn

1 Tausta

Eduskunnan lakivaliokunta on pyytänyt Poliisihallituksen asiantuntijalausuntoa komission tiedonannosta eurooppalaisesta lähestymistavasta tekoälyyn.

Komission tavoite edistää eurooppalaista ihmiskeskeistä ja luottamusta herättävää lähestymistapaa tekoälyyn, sekä tavoitetta luoda Eurooppaan tekoälyn kehittämiselle ja soveltamiselle suotuisa toimintaympäristö nähdään tuettavaksi. Tässä lausunnossa esitettävien näkökulmien ja kehittämisalueiden sääntelyä tulisi tukea EU-tasoisesti ja kansallisesti.

2 Tekoälyn hyödyntämiseen liittyviä näkökulmia ja kehittämisalueita

Suotuisan eurooppalaisen toimintaympäristön rakentamisessa tulisi panostaa erityisesti tietoturvallisen eurooppalaisen infrastruktuurin rakentamiseen. Infrastruktuuri tukee osaltaan tarvelähtöisyyttä, tehokkuutta sekä ketteryyttä. Esimerkiksi eurooppalainen pilvikapasiteettia tarjoava toimija puuttuu markkinoilta, mikä on selkeä puute erityisesti turvallisuustoimijoiden näkökulmasta (vrt. C-311/18, ns. Schrems II -päätös). Panostaminen perustutkimukseen tietotekniikassa ja puolijohdetekniikassa on edelleen avain myös tekoälyn hyödyntämiseen liiketoiminnassa, jotta eurooppalaiset yritykset voisivat saavuttaa globaaleiden toimijoiden etumatkaa suhteessa ohjelmistokomponenttien laskentakyvykkyteen.

Julkishallinnon tulee toimia suunnannäyttäjänä ja edelläkävijänä tekoälyratkaisujen hyödyntämisessä. Eurooppalaisten koalitioiden rakentaminen ja niiden kautta tiedon sekä kokemusten ja parhaiden käytäntöjen jakamisen edistäminen muiden jäsenvaltioiden kanssa on kannatettavaa. Tarkoituksenmukaiseksi nähdään esimerkiksi yhteiseurooppalaisen poliisitoiminnan koalition muodostaminen tiedon ja kokemusten jakamista tukemaan. Yksittäisenä kehityskohteenä tunnistetaan tekoälyratkaisujen tarvitseman luotettavan tekoälyn vaatimusten mukaisen sekä poliisin tarpeeseen tarkoituksenmukaisen koulutusdatan kehittäminen, koska poliisitoimintaan liittyvä tekoälyn koulutusdatan puuttuminen on yksi merkittävä hidaste tekoälyratkaisujen kehittämisessä.

Lisäksi EU:n toimesta voitaisiin hahmotella laatukriteeristöt ja luokittelut tekoälyn käytölle julkishallinnossa tai henkilötietojen käsittelyssä. Esimerkiksi luomalla standardikriteerit koulutusdatan ja verrokkidatan valinnalle sekä tekoälyalgoritmin virheherkkyydelle ko. datalle voitaisiin ratkaisun virheherkkyys ilmoittaa pakollisena tietona esimerkiksi tietojärjestelmän rekisteriselosteessa.

Maailma digitalisoituu tällä hetkellä voimakkaimmin englannin ja kiinan kielellä. Yhtenä teemana EU:n yhteiselle ponnistukselle tekoälyn kehittämisessä olisi keskittyä EU:n monikielisyyden aiheuttamien ongelmien helpottamiseen yritysten ja organisaatioiden toiminnassa. Tämä voi tapahtua lähinnä luonnolliseen kieleen liittyvissä ja niitä tukevissa algoritmeissa sekä datakirjastoissa, kuten esimerkiksi nimistöissä, sanakirjoissa, sanojen perusmuotoon palauttamisissa, taivutusmuodoissa ja sanaluokkien lauserakenteen ymmärtämisissä. Avoimen lähdekoodin työtä tulisi tässä asiassa tukea.

Komission esitys eurooppalaisesta lähestymistavasta tekoälyyn tukee yksityisen ja julkisen sektorin sekä korkeakoulujen yhteistyötä tekoälyratkaisujen kehittämisessä ja käytössä. Turvallisuusviranomaisten tulee mahdollisuuksien mukaan pystyä myös hyödyntämään tällaista innovaatioverkostoa. On poliisitoimen etu, että eurooppalaiset yritykset kehittävät osaamistaan ja kyvykkyyksiään tekoälyn kehityksessä, koska poliisin järjestelmäkehityksessä hyödynnetään vahvasti yritysten osaamista ja tarjontaa.

Tekoälyn hyödyntäminen valtiohallinnossa vaatii myös organisaatioiden välistä yhteistyötä erityisesti resurssipulan vuoksi. Virastojen työtä voi tehokkaimmin tukea yhteisillä kehitykseen tarvittavilla tekoälyalustoilla valtion keskeisten palvelutuottajien toimittamina huomioiden organisaatioiden erilaiset turvallisuusluokitteluvaatimukset.

Tekoälyratkaisuiden ylläpidon ja luotettavan jatkuvuuden varmistamiseksi poliisitoimella tulee olla hallussaan myös omaa osaamista. Erityisesti julkisen sektorin ja turvallisuusviranomaisten kilpailukyvykkyyteen resurssimarkkinoilla tulee panostaa, niin valvonnan kuin teknisten ratkaisuiden toteutuksen osalta.

3 Riskit tekoälyn hyödyntämisen rajoituksiin liittyen

Tekoälyn mahdollisuuksien lisäksi toiminnan laajentumiseen liittyy myös poliisitoimen näkökulmasta riskejä. Onkin erittäin tärkeää kehittää osaamista EU:ssa ja sen verkostoissa, jotta sitä voidaan hyödyntää myös tekoälyavusteisesti tehtyjen rikosten selvittämisessä ja ennaltaehkäisyssä.

Riskinä mainittakoon myös tulevan sääntelyn rajoittavuus lainvalvonnan käyttötarkoitusten osalta, erityisesti liittyen tekoälyn hyödyntämiseen biometrisissa tunnistamistarpeissa. Lainsäädännön ei pitäisi muodostua liian rajaavaksi ja siten EU-alueen sisäisen turvallisuuden ylläpitämisen sekä rikosten ennalta estämisen ja paljastamisen keinoja rajoittavaksi. Lainvalvontakäyttöön tarkoitetuissa järjestelmissä tapahtuvaa tietojenkäsittelyä ohjaavat kansallisen lainsäädännön lisäksi mm. EU:n yleinen tietosuojasetus (GDPR) sekä ns. rikosasioiden tietosuojadirektiivi (EU) 2016/680. Tekoälyä koskeva komission esitys asettuu osin edellä mainittujen normien kanssa

päällekkäin, jonka vuoksi on tärkeää varmistaa, että järjestelmien käyttö ja kehitys sekä tietojenkäsittely on säännelty yhdenmukaisesti.

Tekoälyä hyödyntävien järjestelmien käytöllä voidaan mahdollistaa lainvalvontaviranomaisissa suurten tietomassojen käsittely käyttämättä toimintaan merkittäviä määriä henkilöresursseja. Poliisin toiminnassa suuria tietomassoja käsitellään esimerkiksi laajoissa järjestäytyneen rikollisuuden tai tietoverkkorikollisuuden tutkimisissa. Mikäli lainsäädännöllä rajoitetaan merkittävästi tekoälyä hyödyntävien järjestelmien kehittämistä ja käyttöä rikostorjunnassa, poliisin henkilöressitarpeet tiedon manuaaliselle käsittelylle ovat selvästi suuremmat kuin koneellisella tiedon käsittelyllä. Varsinkin laajoissa tietoverkkoa hyväksikäyttäen tehtyjen rikosten tutkimisessa tietoa voi olla tutkittavana useita petatavuja ja tällaisen tiedon läpikäynti sekä relevantin tiedon löytäminen manuaalisesti voi olla erittäin vaikeaa tai mahdotonta jatkossa ilman tekoälyä hyödyntävää järjestelmää.

Eurooppalainen lähestymistapa tekoälyyn vaatii lisäksi mittavaa rahoitusta, joka on otettava huomioon myös kansallisesti. Erityisesti julkisen hallinnon kriittisten investointien ja infrastruktuurin kehittämisen taloudellisten vaikutusten näkökulmasta tavoitteet on syytä suunnitella julkisen talouden suunnitelmaan ennakoivasti. Rikostorjunnan kannalta merkittäviä tulevaisuudessa tekoälyä hyödyntäviä järjestelmiä ovat biometrisen tunnistamisen järjestelmien lisäksi myös rikosanalyysiin liittyvät järjestelmät. Asetusehdotuksen liitteessä III on kuvattu kriteerejä, joiden perusteella tekoälyä hyödyntävä järjestelmä voidaan lukea korkean riskin järjestelmäksi. Osa lainvalvontaviranomaisten käytössä tai kehitteillä olevista järjestelmistä esim. rikosanalyysissä tai todisteiden tutkimisessa luokitellaan korkean riskin järjestelmiksi. Korkean riskin järjestelmien kehittämistä ja käyttöä koskevat vaatimukset aiheuttavat kustannuksia viranomaisille ja kustannusten nousu voi aiheuttaa sen, että uusinta teknologiaa hyödyntävien järjestelmien hankinta ei ole mahdollista resursseista johtuvista syistä. Lainsäädännön jatkovalmistelussa tulisi erityisesti kiinnittää huomiota ehdotuksen realististen taloudellisten ja hallinnollisten vaikutusten selvittämiseen, jotta poliisi voisi myös tosiasiallisesti hyödyntää tekoälyjärjestelmiä. Oletettavissa kun on, että komission suunnitelmat yritysten tukemisesta tekoälyä hyödyntävien järjestelmien käytössä eivät todennäköisesti koskisi viranomaisten toiminnan tukemista.

Sen sijaan, että esitettäisiin lainvalvonnalle muita toimijoita tiukempia rajoituksia erilaisten järjestelmien kehitykselle ja käytölle olisi tarpeen varmistaa, että tekoälyä voidaan hyödyntää perusoikeuksia kunnioittavasti säätämällä henkilötietojen käsittelystä teknologianeutraalisti, kuten on tehty GDPR:ssä ja rikosasioiden tietosuojadirektiivissä. Asetusesityksen liitteessä III mainitut kriteerit korkean riskin järjestelmille kattavat nykyisellään merkittävän osan lainvalvontaviranomaisten suorittaman rikostorjunnan tehtävistä, joissa tekoälyä hyödyntävillä toimilla voitaisiin taata viranomaisten laadukas, tehokas ja oikeusvarma toiminta käyttämättä toimintaan merkittävää määrää manuaalista työtä. Tekoälyavusteiset järjestelmät voivat parhaimmillaan tukea poliisin työtä esimerkiksi rikostorjunnassa, mutta lopullinen päätöksenteko ja vastuu toimenpiteiden suorittamisesta on aina tehtävää hoitavalla virkamiehellä.