

Viite: VNS 7/2025 vp

Asiantuntijalausunto tulevaisuusvaliokunnalle tekoälyn hyödyntämisen uhkista ja mahdollisuuksista informaatiovaikuttamiseen ja yhteiskunnan vakauteen liittyen

Tulevaisuusvaliokunta on pyytänyt Liikenne- ja viestintävirastolta sekä Traficommin Kyberturvallisuuskeskukselta kirjallista ja suullista lausuntoa valtioneuvoston tulevaisuusselonteon ensimmäisestä osasta, Strateginen toimintaympäristöanalyysi sekä skenaarioita vuoteen 2045. Tarkempi teema pyydytyissä asiantuntijalausunnoissa sekä kuulemisessa on tekoälyn uhat ja mahdollisuudet. Liikenne- ja viestintävirasto kiittää mahdollisuudesta lausua asiassa ja lausuu selonteosta sekä teemasta seuraavaa:

1 Tekoälyn murros ja käyttöönoton epävarmuudet

Tekoälyn tekniikassa on meneillään vallankumous, jolla on suuri potentiaali muuttaa perustavanlaatuisella tavalla työntekoa ja yhteiskuntaa laajemminkin. Tekoälyn laajempaan käyttöönottoon sisältyy merkittäviä epävarmuustekijöitä. Tästä huolimatta tekoälyyn varhaisessa vaiheessa panostavat tulevat todennäköisesti hyötymään eniten.

Generatiivisen eli sisältöä tuottavan tekoälyn vahvuutena on asiayhteyksien ja rakenteiden hahmottaminen sille annetusta materiaalista, ja vastaavan sisällön tuottaminen. Tekoälyjärjestelmät voivat myös komentaa muita ohjelmistoja. Näillä peruskyvykkyyksillä on rakennettu laajempia järjestelmiä, joista monimutkaisimmat agenteiksi kutsutut järjestelmät toimivat myös itsenäisesti.

Tekoälyn kehitys on ollut nopeaa ja sen etenemisen ennakointi on ollut vaikeaa. Ohjelmistojen tuotannossa käynnissä oleva muutos voi kuitenkin antaa suuntaa sille, kuinka tekoäly tulee muuttamaan muitakin työnkuvia.

1.1 Käyttöönoton kehityspolku: asiantuntijatyöstä arjen työkaluksi

Tekoälyn käyttöönotto etenee tyypillisesti vaiheittain. Ensimmäisessä vaiheessa jonkin työnkulun muuttaminen tekoälyllä vaatii tehokkaimpien järjestelmien käyttöä ja käyttäjältä merkittävää asiantuntemusta. Vähitellen samat kyvykkyydet tuodaan vähätehoisempiin tekoälyjärjestelmiin ja asiantuntemusvaatimukset vähenevät. Lopulta tekoälyjärjestelmät voivat toimia riittävän laadukkaasti myös itsenäisinä tekoälyagentteina.

Monien johtavien ohjelmistovalmistajien tulevaisuuden suunnitelmissa tekoälyn roolia pidetään itsestään selvänä. Ihmisten rooli muuttuu vähitellen

ohjelmistojen toteuttajasta tekoälyjärjestelmien ohjaajiksi ja korkeamman tason suunnittelijoiksi.

Tämä ei kuitenkaan välttämättä tarkoita, että työ ohjelmistotalalla vähenisi. Kun ohjelmistotuotanto tulee saataville laajemmalle käyttäjäkunnalle, tarpeet ohjelmistoille voivat päinvastoin kasvaa. Työn tekemisessä vaadittavat taidot muuttuvat, ja tarpeet elinikäiselle oppimiselle ennestään kasvavat. Yksinkertaisten työvaiheiden automatisointi voi muodostua esteeksi nuorempien työntekijöiden alalle pääsyyn, ja väliinputoaminen on vaarana muullakin työvoimalla.

1.2 Rajoitteet ja epäonnistumisen riskit

Tekoälyn käyttöönotto ei kaikilta osin tule sujumaan menestyksekkäästi. Jos työtehtävästä ei ole saatavilla riittävästi tekoälylle soveltuvaa opetus- ja esimerkkimateriaalia, generatiivinen tekoäly ei ole hyvä ratkaisu. Esimerkkinä voidaan mainita työtehtävät, jotka edellyttävät hiljaisen tiedon omaksumista.

Uutisoinnin perusteella monet tekoälyprojektit epäonnistuvat jo epämääräisten tavoitteiden vuoksi. Monia tietotyön tehtäviä voisi tehostaa paremmin perinteisellä ohjelmistoautomaatiolla.

Tekoälyjärjestelmien käyttöönotto vaatii muutoksia myös muihin organisaation käyttämiin järjestelmiin. Yksinkertaistaen voi sanoa, että nykyiset tietojärjestelmät on tehty ihmiskäyttäjää varten, ja tulevaisuudessa samat järjestelmät suunnitellaan tekoälyn käytettäväksi. Nämä muutokset voivat kuitenkin viedä vuosia, mikä hidastaa monien tekoälyjärjestelmien käyttöönottoa.

1.3 Kyberturvallisuus: uudet hyökkäyspinnat ja puolustuksen tarve

Nykyisissä tekoälyjärjestelmissä on myös paljon puutteita. Tekniikka ja tekoälyn käyttöä koskeva sääntely on vielä nuorta ja kehitettävää on paljon. Päivittäin julkistetaan varoittavia esimerkkejä tekoälyn käytön ongelmista. Osassa tapauksissa kyse on parhaiden käytäntöjen vastaisesta käytöstä tai suuren riskin käyttötapauksista. Moniin tekoälyjärjestelmien käyttötapauksiin on pyritty vastaamaan myös sääntelyn keinoin EU:n uudessa tekoälyasetuksessa.

Nykyisissä tekoälyjärjestelmissä on myös kyberturvallisuusongelmia, joista osa on rakenteellisia. Tekoälyn kestävä käyttö vaatiikin jatkuvia panostuksia sekä tekoälyn puolustamisen että tekoälyn puolustuksellisen käytön kehittämiseksi. Tekniikan kypsyessä kyberturvallisuuspuutteisiin löydetään tyypillisesti vähitellen ratkaisuja. Tässä voi kuitenkin kestää vuosia. Muutosnopeuden vuoksi vanhoja järjestelmiä joudutaan myös korjaamaan vuosien ajan.

1.4 Informaatiovaikuttaminen: kustannusten lasku ja vaikutusympäristön kuormittuminen

Sisältöä tuottavat tekoälyjärjestelmät ovat jo tulleet merkittäväksi osaksi verkon sisällöntuotantoa sekä ihmisten tapaa hakea ja käsitellä tietoa. Tekoälyjärjestelmien voidaan siis katsoa käyttävän merkittävää valtaa informaatioympäristössä. Vaikutukseltaan tätä valtaa voidaan verrata esimerkiksi hakukoneiden ja sosiaalisen median alustojen taustalla olevien algoritmien valtaan.

Osa tämän hetken tekoälyjärjestelmistä on avoimen puolueellisia tai niitä on helppo käyttää informaatioympäristöä vinouttavalla tavalla. Pahimmillaan tekoäly voi vahvistaa kuplautumista, kun sisältöä kohdennetaan yhä tarkemmin käyttäjän ennako-oletusten mukaiseksi

Tekoälyllä tuotettuun verkkosisältöön liittyy useita ongelmia. Tekoälyn avulla voidaan toteuttaa informaatiovaikuttamista aiempaa pienemmillä kustannuksilla, mikä lisää vaikuttamisen määrää, tekee siitä monipuolisempaa ja tuo kentälle uusia toimijoita. Samalla automaattisesti tuotetun sisällön määrän kasvu hankaloittaa käyttäjien tiedonhakua. Jos käyttäjä ei löydä haluamaansa sisältöä, verkon arvo ja käytettävyys voivat heikentyä.

1.5 Läpinäkyvyys, merkinnät ja aitoustodentaminen

Ratkaisuksi tekoällysisällön tuomaan ongelmaan on esitetty tekoällysisällön selkeää merkitsemistä. Monet verkon toimijat ovat ottaneet käyttöön näitä merkintöjä oma-aloitteisesti, ja teknisiä keinoja aidon sisällön merkitsemiseksi kehitetään. EU:n tekoälyasetus tulee velvoittamaan läpinäkyvyyteen tekoällysisällön merkitsemisessä. Tämän säädännön toteuttamisella ja valvonnalla voi olla suuri merkitys verkon käytettävyyteen tulevaisuudessa.

Myös rikolliset ovat ottaneet käyttöön tekoälyn huijausten tuottamisessa. Tekoälyllä on toteutettu väärennettyä tekstiä, kuvaa, ääntä ja videota entistä uskottavammissa huijauksissa. Tekoälypersoonat tulevat todennäköisesti olemaan arkipäivää tulevaisuudessa, ja myös niitä tullaan käyttämään laajalla mittakaavalla huijauksissa.

Huijauksia voidaan torjua edellä mainituilla teknisillä aitoustodistuksille valokuva- ja videosisällölle. Tällaisen tekniikan käyttöönotto tulee kuitenkin todennäköisesti olemaan hidasta. Aitouden lisäksi keskeistä on arvioida sisällön lähteen entistä tarkempaa todentamisen mahdollisuutta.

1.6 Oikeudelliset ja vastuukysymykset yhteiskunnan vakauden näkökulmasta

Tekoälyagenttien toiminta tulee johtamaan myös hankaliin oikeudellisiin kysymyksiin, jotka liittyvät muun muassa tekoälyjärjestelmien päätöksentekoon

käyttäjiensä puolesta, tekoälyjärjestelmän arviointiin itsenäisenä toimijana sekä tekoälyjärjestelmien läpinäkyvyyteen. Vastuukysymysten ratkaiseminen tekoälyjärjestelmien keskisessä automaattisessa toiminnassa voi olla monimutkaista. Onko vastuu väärästä toiminnasta järjestelmän valmistajalla, integraattorilla vai käyttäjällä? Minkälaisia päätöksiä on hankala hyväksyä tekoälyn toteuttamina?

1.7 Mahdollisuudet: tehokkuus, paikallinen tekoäly ja eurooppalainen liikkumavara

Tekoälyjärjestelmillä on suuria taloudellisia ja yhteiskunnallisia mahdollisuuksia. Julkisessa keskustelussa keskitytään usein johtaviin tekoälyjärjestelmiin ja niiden kehitykseen valtaosin Euroopan ulkopuolella. Saatavilla olevat avoimet tekoälyjärjestelmät mahdollistavat kuitenkin jatkuvasti enemmän erilaisia käyttötarkoituksia. Tulevaisuudessa suurimmassa osalla järjestelmiä voidaan käyttää paikallista tekoälyä toiminnan tehostamiseen. Tämä avaa Suomelle ja Euroopalle uudenlaisia mahdollisuuksia myös uniikin liiketoiminnan tuottamiselle. Euroopassa ja EU:ssa on edellä mainitusti rakennettu myös maailman ensimmäisiä sääntelykehikoita tekoälyjärjestelmille sekä niiden sallitulle käytölle EU:n tekoälyasetuksessa. Tekoälyn avulla myös julkishallinnon toimintaa voidaan kehittää eri tavoilla, jotka muuttavat prosesseja, työnteon tapaa, tehokkuutta ja rakenteita.

2 Tulevaisuusskenaariot ja mahdollisuudet: tekoälyagentit julkishallinnossa, luottamus ja vakaus

Julkishallinnossa teknologian käyttöönotto onnistuu vain, jos se vahvistaa luottamusta. Kansalaisten luottamus hallintoon on digitaalisten uudistusten onnistumisen keskeinen edellytys, ja luotettavat, reagoivat ja oikeudenmukaiset palvelut voivat vahvistaa luottamusta. Tekoälyagenttien kohdalla luottamuksen merkitys korostuu, koska niiden toiminta on usein monivaiheista ja vaikeammin hahmotettavaa kuin perinteinen ennalta määritettyihin sääntöihin perustuva automaatio.

Oikeusturvan näkökulmasta kriittistä on ratkaisujen perusteiden jäljitettävyydestä tiedot ovat peräisin, mitä sääntöjä on sovellettu, missä kohdin on tehty harkintaa ja kuka harkinnan on tehnyt. Tekoälyagenttien käyttö ei poista vastuuta – päinvastoin se korostaa tarvetta määritellä vastuut, hyväksynnit, valvonta ja poikkeamien käsittely selkeämmin kuin aiemmin.

Yhteiskunnan laaja digitalisoituminen lisää riippuvuutta datasta, automaatiosta ja reaaliaikaisesta tilannekuvasta. Yksityisen sektorin lisääntyvä tekoälyn käyttöönotto voi johtaa kasvavaan viranomaisasiointitarpeeseen. Tekoälyagentit voivat parantaa palvelujen saatavuutta, tehokkuutta ja vaikuttavuutta sekä vahvistaa luottamusta julkiseen hallintoon, jos niiden käyttö on läpinäkyvää,

turvallista ja eettisesti hallittua. Samalla paineet tuottavuuden, turvallisuuden ja taloudellisen kestävyys suhteen kasvavat, mikä korostaa turvallisuutta perusedellytyksenä: uusien ratkaisujen on oltava tietoturvallisia, yksityisyyttä kunnioittavia ja vastuullisesti johdettuja, jotta kansalaisten luottamus säilyy.

Kansalaisnäkökulmasta tekoälyagentit voivat tarjota ympärivuorokautisia digitaalisen palveluja. Yksi keskusteleva rajapinta voi ohjata oikeaan palveluun, täyttää hakemuksia ja vastata kysymyksiin ilman, että kansalaisen tarvitsee ymmärtää hallinnon organisaatorakennetta. Tämä voi lisätä palvelujen saavutettavuutta, nopeuttaa asiointia ja vahvistaa luottamusta julkisiin palveluihin.

Agentit yleistyvät erityisesti asiakaspalvelussa, hakemusprosessien valmistelussa, tiedonhaussa ja tilannekuvan muodostamisessa. Ihmisen rooli painottuu ohjaukseen, valvontaan ja harkintaa vaativiin ratkaisuihin. Tämä malli voi tuottaa huomattavia hyötyjä, mutta edellyttää toimintamalleja, joissa agenttien toiminta on tarkastettavaa ja poikkeamat hallittavissa.

2.1 Tulevaisuusnäkökulma: tekoäly osaksi perusinfrastruktuuria ja järjestelmäriskien kasvu (2030–2045)

Vuoteen 2035 mennessä tekoäly on ketjutettu tuotantoprosessi, joka ulottuu datasta tekoälyjärjestelmien koulutukseen, rajapintapalveluihin, koodaus-agentteihin ja integraatioihin kriittisiin liiketoiminta- ja viranomaisjärjestelmiin. Tekoälypalvelut ovat usein jatkuvassa, automaattisessa tuotantokäytössä ja nojaavat kalliiseen laskentaan, mikä muuttaa niiden turvallisuusluonnetta perustavanlaatuisesti.

Tekoälyinfra on altis palvelunestohyökkäyksille. Palvelu voidaan lamauttaa ilman perinteistä tietomurtoa kuormittamalla laskentaa tai nostamalla käytöstä syntyvät kustannukset kestäättömiksi. Moderneissa järjestelmissä riskin paionpiste on siirtynyt yksittäisistä palveluista ja palvelimista keskitettyihin hallintakerroksiin. Jos hallintataso murretaan, koko tekoäly-ympäristö on käytännössä hyökkääjän hallinnassa.

2.2 Itseään kehittävät järjestelmät ja koodiagentit: hallinnan raja voi siirtyä organisaation ulkopuolelle

Koodausagentit kykenevät itsenäisesti tuottamaan, testaamaan ja kehittämään tuotantokoodia. Tulevaisuudessa myös järjestelmäkokonaisuudet kehittyvät osin ilman suoraa ihmiskontrollia. Keskeinen epävarmuus ei ole se, kehittykö tekoäly, vaan tapahtuuko siirtymä hallitusti vai syntyykö katkospiste, jossa osa toimijoista jää pysyvästi jälkeen – ja samalla myös turvallisuuskäytännöt ja arkkitehtuurit vanhenevat.

Samanaikaisesti hyökkäyskyvykkyydet demokratisoituvat: avoimet agenttiratkaisut mahdollistavat yhä kehittyneempien hyökkäysten toteuttamisen matalalla kynnyksellä ja massiivisesti rinnakkaistettuna. Tämä kasvattaa riskiä siitä, että hyökkäysvolyymi ja -nopeus ylittävät puolustuksen kapasiteetin rakenteellisesti, ellei puolustus automatisoidu ja skaalaudu samassa tahdissa.

2.3 Tekoälyn systeemiset riskit: keskittyminen, riippuvuudet ja ketjureaktiot

Tekoälypino rakentuu usein useista kansainvälisistä ja toisiinsa kytkeytyvistä osista: pilvipalveluista, kiihdytinlaitteista, järjestelmätoimittajista, avoimen lähdekoodin komponenteista sekä dataketjuista. Riippuvuuksien ketjut pitenevät ja monimutkaistuvat, jolloin toimitusketjun yhden lenkin häiriö tai murto voi laajentua järjestelmätason häiriöksi. Erityisen kriittinen on hallintatason tietomurto, joka voi antaa samanaikaisen pääsyn tekoälyjärjestelmään, dataan ja laskentakapasiteettiin, sekä mahdollisuuden peittää jäljet.

Keskittyminen muutamaan suureen toimijaan kasvattaa monokulttuuririskiä: yhden toimittajan häiriö, päivitys tai päätös voi kertautua kymmeniin tai satoihin prosesseihin useilla sektoreilla yhtä aikaa. Teknologiset vaikuttavat riskiprofiiliin. Avoimien järjestelmien voi vähentää toimittajalukkoa ja lisätä läpinäkyvyyttä, mutta samalla helpottaa laajamittaista väärinkäyttöä. Suljettujen järjestelmien käyttö taas kasvattaa keskittymis- ja riippuvuusriskiä.

Kun tekoäly kytkeytyy lähemmäs fyysisiä prosesseja (energia, logistiikka, teollisuus), digitaalinen häiriö voi muuttua aiempaa helpommin fyysiseksi tai yhteiskunnalliseksi häiriöksi. Tämä nostaa yhteiskunnan vakauden kannalta keskiöön resilienssin, jatkuvuuden ja palautumiskyvyn – ei vain yksittäisten järjestelmien tietoturvan.

2.4 Disruptiivinen muutos: tarveperusteiset ohjelmistot ja jatkuvasti muuttuvat järjestelmät

Tekoäly voi muuttaa markkinarakenteita siten, että ohjelmistokehitys siirtyy kohti on demand -mallia, jossa sovelluksia ja järjestelmiä generoidaan lennosta agenttien avulla. Tällöin pysyvien ohjelmistotuotteiden merkitys voi vähentyä, ja keskeisiksi tuotannon tekijöiksi nousevat vaatimukset ja tekniset määrittelyt, ohjelmistoekosysteemit ja laskentakapasiteetin saatavuus. Samalla painopiste siirtyy yksittäisistä sovelluksista kohti jatkuvasti oppivia ja mukautuvia järjestelmiä, jolloin turvallisuus ja vastuu eivät voi perustua pistemäisiin tarkastuksiin vaan jatkuvaan varmistamiseen ja valvontaan.

3 6G-verkot tekoälyjärjestelmien selkärankana ja Suomen kilpailukyvyn edistäjänä

6G on strateginen murroskohta, jossa määritellään uudelleen viestintäverkkojen arkkitehtuuri ja samalla se, mihin tekoäly sijoittuu yhteiskunnan perusinfrastruktuurissa. Kyse ei ole ensisijaisesti nopeudesta tai kapasiteetista, vaan siitä, kuka kontrolloi älykkyyttä, missä päätöksiä tehdään ja millaiseksi järjestelmien resilienssi ja turvallisuus muodostuvat. 6G yhdistää tietoliikenteen, laskennan, tekoälyn, pilvipalvelut, satelliittijärjestelmät ja fyysisen maailman havainnoinnin yhdeksi reaaliaikaiseksi kokonaisuudeksi: verkko ei enää vain välitä dataa, vaan osallistuu sen tulkintaan ja käyttöön.

Tämä kehitys vie kohti verkkoja, jotka tekevät yhä enemmän päätöksiä itsenäisesti. Turvallisuuskulmasta uudet uhat kohdistuvat tällöin yhä useammin verkon toiminnalliseen logiikkaan (tekoälyn manipulointi, päätöksenteon läpinäkyvättömyys, virheiden ketjuuntuminen) eikä pelkkään tiedonsiirtoon. Lisäksi 6G:n ohjelmistopohjaisuus, virtualisointi, monitoimittajaympäristöt ja avoimet rajapinnat sekä pilvi- ja satelliitti-integraatiot kasvattavat kokonaisuuden monimutkaisuutta ja riippuvuuksia.

3.1 Strateginen mahdollisuus: hajautettu ja turvallisuutta painottava eurooppalainen tekoälyinfra

6G:n ja telekommunikaatioteknologioiden kautta EU:lla – ja erityisesti Suomessa – on mahdollisuus vaikuttaa siihen, rakennetaanko tekoälyn infrastruktuuri keskitettyjen alustojen varaan vai hajautetummin lähemmäs sensoreita, päätelaitteita ja fyysisiä prosesseja. Hajautus voi vähentää riippuvuutta keskitetystä pilvilaskennasta, pienentää viiveitä ja parantaa häiriönsietokykyä, mutta se edellyttää, että turvallisuus, hallinta ja valvonta suunnitellaan arkkitehtuuriin sisään. 6G-tekniikan kaksikäyttöluonne korostaa standardoinnin, varautumisvelvoitteiden ja turvallisuusohjauksen merkitystä.

4 Lopuksi

Liikenne- ja viestintävirasto korostaa, että Suomen tulee vaikuttaa tekoälyratkaisujen - ja palveluiden kansainväliseen kehitykseen niin uusien mahdollisuuksien hyödyntämiseksi kuin uhkien torjumiseksi. Tätä vaikuttamista tarvitaan niin uuden EU-tason tekoälysäätelyn mahdollisimman tehokkaaksi täytäntöönpanemiseksi kuin myös uusien teknologioiden sekä tekoälyjärjestelmien käytötapausten tunnistamiseksi sekä kehittämiseksi. Suomessa ja Euroopassa kehitetään sekä langatonta viestintäteknologiaa että niitä hyödyntäviä sovelluksia, joissa tekoäly on jo tällä hetkellä tärkeä mahdollistaja. Liikenne- ja viestintävirasto korostaa, että tekoäly tarvitsee erityisesti korkean riskin käyttötapauksissa selkeät riski- ja turvallisuuskontrollit. Näiden osalta on syytä huomioida, että tarkoituksena ei ole hidastaa arkisten prosessien tehostamista tai ihmisen

päätöksentekoa tukevien sovelluksien kehitystä, vaan varmistaa käyttöönotettavien teknologioiden sekä näihin perustuvien palveluiden turvallisuus riskiperustaisesti.

Liikenne- ja viestintävirasto Traficom
PL 320
000059 TRAFICOM
Puh. 029 534 5000
traficom.fi