Tekoäly lukee, kirjoittaa ja keskustelee

Tulevaisuusvaliokunnan lausuntopyyntö

Asia: E 62/2021 vp Valtioneuvoston selvitys: Komission tiedonanto: Tiedonanto eurooppalaisesta lähestymistavasta tekoälyyn

Asia E 48/2021 vp Valtioneuvoston selvitys: Komission tiedonanto: 2030 digitaalinen kompassi: eurooppalainen lähestymistapa digitaalista vuosikymmentä varten

Asia: E 86/2021 vp Valtioneuvoston selvitys: Ennakkovaikuttaminen: Euroopan unionin datasäädös

Asia: U 28/2021 vp Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi tekoälyn harmonisoiduksi sääntelyksi (Artificial Intelligence Act)

Turussa 27.10.2021

Tapio Salakoski
Professori, tietojenkäsittelytiede
Dekaani, matemaattis-luonnontieteellinen tiedekunta
Turun yliopisto

Sisällys

Tekoäly lukee, kirjoittaa ja keskustelee 3

Mistä on kyse? 3

Puhe ja teksti 3

Kieli ja kielimallit 4

Kieliteknologian käyttötapoja 4

Tiedonhaku 4

Sisältöanalyysi 5

Tekstin tuottaminen ja vaikuttaminen 5

Tukiäly ja tietoisuus 6

Tekoäly muutosvoimana 6

Kielten asema 6

Digitalisaation tehostuminen 6

Yksityisyys, väärinkäytökset, valvonta ja vaikuttaminen 7

Viestit päättäjille ja kansalaisille 7

Huippuosaaminen ja yleissivistys 7

Sääntely vs. kilpailukyky 7

Kokonaisturvallisuus 7

Tekoäly lukee, kirjoittaa ja keskustelee

Ihmisen kieli on ihmisen mieli; kieli on korkeamman ajatustoiminnan ja kommunikoinnin luonnollinen väline. Rakenteinen, numeerisesta tai valmiiksi luokitellusta tiedosta koostuva data ei riitä, vaan tarvitaan myös kuvaa, ääntä – ja vapaata tekstiä. Jotta faktat saavat merkityksensä, ne on asetettava kontekstiin: tarina on välttämätön ymmärtämiselle ja oppimiselle. Ihmisen kieli puhuttuna kielenä syntyi ryhmän sisäisen kommunikaation tarpeeseen. Tarve kielellisen informaation pysyvään tallentamiseen synnytti sittemmin kirjoitetun kielen, kirjoitusasun lukuisille puhutuille kielille. Kirjapainotaito aiheutti kulttuurisen vallankumouksen ja synnytti modernin sivistyksen.

Koneen kykyä ymmärtää ja tuottaa luonnollista kieltä pidetään koneen älykkyyden olennaisena osana. Sitä tutkiva tekoälyn haara on **kieliteknologia** eli **luonnollisen kielen käsittely** (Natural Language Processing, NLP). 1900-luvun puolivälissä kielen kääntämisessä odotettiin tekoälyn nopeata läpimurtoa. Tehtävä osoittautui paljon luultua vaikeammaksi, ja luonnollista kieltä alettiin pitää voittamattomana haasteena tietokoneelle. Nyt kuitenkin kieliteknologian läpimurron aika on käsillä. Viime vuosien nopean kehityksen takana on tietokoneiden laskentatehon ja datan määrän kasvu sekä paradigman muutos. Perinteisestä lingvistisen mallintamisen lähestymistavasta on siirrytty koneoppimiseen ja massiiviseen dataan perustuvaan kieliteknologiaan.

Mistä on kyse?

Kieliteknologiaa kehitetään kielen käytön eri osa-alueilla ja sovelletaan useisiin tehtäviin. Seuraava jäsennys ei ole tyhjentävä, mutta antaa kuvan kielen keskeisestä merkityksestä dokumentoidun tiedon kentässä ja kieliteknologian monipuolisuudesta.

Puhe ja teksti

Tämä kirjoitus keskittyy kirjoitettuun kieleen. Puhuttua kieltä voidaan pitää kielen alkuperäisenä muotona, mutta sivistyksen perustana on kirjallinen dokumentaatio. Puheen käsittely on oma tutkimushaaransa, mutta sen tietosisällön käsittely palautuu kirjoitettuun kieleen. Puhe sisältää sanallisen sisällön ohella muutakin kommunikaatiota, äänensävyn, painotusten ja rytmityksen välittämää informaatiota, kuten tunteita. Näiden välittämiseen puheessa liittyvät oleellisesti myös kasvojen ilmeet ja kehon kieli. Kehon kieltä käytetään myös sanallisen sisällön välittämiseen viittomakielten avulla.

Puhuttu kieli on myös aina sidoksissa puhujaan: se ei ole anonyymiä, vaan puhesignaalissa kuuluvat puhujan biometriset ominaisuudet. Puhetta voidaan jopa käyttää luotettavasti puhujan tunnistukseen samaan tapaan kuin sormenjälkiä, silmiä tai kasvoja.

Puhetta käsitellään tulkitsemalla vastaanotettu akustinen puhesignaali sanalliseksi informaatioksi **tekstittämällä** (Speech to Text). Sanallisen tietosisällön analyysi tapahtuu tekstimuotoiselle datalle kehitetyillä menetelmillä. Puheen tuottaminen puolestaan tapahtuu tekstimuotoisen kielen generoinnin jälkeisellä **puhesynteesillä** (Text to Speech). Sovelluskohteita on lukuisia, ja jopa kohtalainen dialogi on mahdollista.

Kieli ja kielimallit

Moderni datalähtöinen NLP perustuu **koneoppimiseen**. Uudet tehokkaat koneoppimisalgoritmit vaativat toimiakseen hyvin suuria datamääriä. Tietokone oppii kieltä kuin ihmislapsi: esimerkkien avulla, toistojen kautta. Puhutut sanat opitaan tunnistamaan ja lausumaan harjoittelun avulla, ja sanojen merkitys täsmentyy niiden esiintyessä yhä uudestaan erilaisissa konteksteissa. Mekanismi on kuin ihmisellä: lukeminen parantaa kielen ymmärrystä, laajentaa sanavarastoa ja vahvistaa ilmaisukykyä.

Kieli voidaan jakaa kielioppiin (**syntaksi**; vastaa kysymykseen miten?), merkitykseen (**semantiikka**; mitä?) ja tarkoitukseen (**pragmatiikka**; miksi?). Lauseiden rakenteen ymmärtäminen ja sanojen tuntemus on välttämätöntä merkityksen ymmärtämiselle. Nykyään kone hallitsee syntaksin hyvin ja kykenee yhä useammin hyödyllisen tasoiseen semanttiseen ymmärrykseen. Luonnollinen kieli on kuitenkin vivahteikasta ja monimerkityksistä. Siksi kielen käyttäjän todellisen tarkoituksen ymmärtäminen on ihmisellekin haastavaa ja pragmatiikka tekoälylle useimmiten vielä liian vaikeata.

Kirjoitetuilla kielillä on erityispiirteensä, mutta niillä on myös yhteisiä ominaisuuksia. Uusimpien tekoälymenetelmien kyvykkyys perustuu massiivisesta datasta opittuihin **kielimalleihin**. Ne kiteyttävät kielellisen osaamisen, joka voidaan rajoitetusti siirtää sovelluksesta ja jopa kielestä toiseen. Kielen kääntäminen oli ennen kokonaan ihmisen erikoisosaamista, mutta nykyään koneen tekemä raakakäännös toimii hyvänä pohjana.

Vaaditun datan ja laskennan suuren määrän vuoksi kielimallien tuottaminen maksaa paljon, joten ne ovat myös kaupallisesti arvokkaita. Niiden hyvyys riippuu opetusdatan määrästä ja laadusta. Algoritmien monimutkaisuuden vuoksi mallit ovat heikosti selitettävissä: kielimalli on 'musta laatikko', jota voidaan arvioida vain tulosten perusteella. Tulosten luotettavuus palautuu vahvasti opetusdataan: määrän kasvattaminen parantaa tuloksia. Myös laadulla on väliä: esimerkkidatasta opitaan samanarvoisesti kaikki sen piirteet, ei pelkästään niitä, joita tavoitellaan. Jos ja kun opetuksessa käytetyt tekstit sisältävät syrjiviä piilomerkityksiä ja jopa epätotuuksia, nekin opitaan.

Kieliteknologian käyttötapoja

Tiedonhaku

Erilaiset hakutoiminnot ovat yleisimpiä NLP:n käyttötapoja. Avainsanahausta ollaan siirtymässä kohti vapaan tekstin käyttöä ja monikielisyyttä. Tekstejä voidaan **luokitella** ennalta annettuihin luokkiin sisällön mukaan tai **ryhmitellä** niiden samankaltaisuuksiin perusteella. Yksityisten ihmisten suorittamat haut ovat niin yleisiä, että niitä voidaan itsessään käyttää datana esimerkiksi epidemioiden leviämistä selvitettäessä.

Muun muassa terveydenhuollon sovelluksissa hakua usein tehostetaan **rakenteistamalla** tekstiä etukäteen annetuin avainsanoin tai otsikoin. Muuttuvassa ja epävarmassa maailmassa luotettavimman ja tarkimman tuloksen tuottaa vapaa tekstihaku: alkuperäinen teksti voidaan jäsentää tai otsikoida myöhemmin uudestaan halutulla tavalla, ja siksi se tulisikin aina säilyttää rakenteistetun dokumentaation rinnalla.

Sisältöanalyysi

Tekstin sisällöllinen analysointi perustuu samankaltaisuuksien, eroavaisuuksien, riippuvuuksien, trendien ja muiden heikkojen signaalien tunnistamiseen. Menetelmiä käytetään diagnostiikan tukena terveydenhuollossa, mutta myös kuluttajien käyttäytymisen selvittämiseksi ja siihen vaikuttamiseksi mainosrahoitteisen toiminnan ja politiikan piirissä. On huomattava, että esimerkiksi Facebookin käyttäjät eivät ole palvelun asiakkaita, vaan myytävä tuote; asiakkaita ovat mainostajat ja muut tahot, jotka ostavat käyttäjäprofiileja toimintansa kohdentamiseksi ja tehostamiseksi. Vastaavaa toimintaa nähtiin Yhdysvaltain presidentinvaaleissa ja Britannian brexit-äänestyksessä.

Tekstin tiivistäminen ja yhteenvedot, tuotteiden ja palvelujen suosittelujärjestelmät sekä päätöksenteon tuki ovat esimerkkejä sovelluksista, jotka vaativat tekstin syvempää sisällöllistä ymmärtämistä. Laadultaan parantunut konekääntäminen on tulossa reaaliaikaiseen kuluttajakäyttöön. Kasvavia sovellusaloja ovat terveydenhuolto ja kauppa, vakuutus- ja rahoitusala sekä viranomaispalvelut kuten patentit ja verotus.

Niin yritykset kuin yhteiskunnalliset tai valtiolliset toimijat ovat kiinnostuneita tekstin aiheen tai aihepiirin, sentimentin (tunnetilan) tai sen vaikutuksen kohteen tunnistamisesta: tarvetta on vihapuheen tunnistamiselle, yrityskuvan kehityksen seurannalle, poliittisen aloitteen suosion arvioinnille tai päätöksen vaikutusten kohdentumisen ennakoinnille. Myös kirjoittajan profilointi tai jopa tunnistaminen voi tulla kyseeseen esimerkiksi historiantutkimuksessa, rikostutkinnassa tai turvallisuusvalvonnassa.

Käyttökohteiden arkaluonteisuuden ja yksityisyydensuojan vaarantumisen vuoksi menetelmien käytön sääntely on erityisen tärkeätä, mutta mallien monimutkaisuuden vuoksi niiden tarkka kontrolli vaikeata. Esimerkiksi Google pyrkii sensuroimaan hakutuloksistaan loukkaavaksi miellettyä sisältöä ja tuottaa samalla systemaattisen vääristymän, minkä vuoksi etniset ja seksuaalivähemmistöt ovat tuloksissa aliedustettuina.

Tekstin tuottaminen ja vaikuttaminen

Kielen tuottaminen on luovaa toimintaa, ja puheen tai tekstin tuottaminen tekoälyn avulla vaatii tekoluovuutta. Automaattisen kielengeneroinnin avulla kyetään nopeuttamaan ja laajentamaan tiedonjakoa, tehostamaan viestin perillemenoa, korjaamaan puhujan omia vajavaisuuksia tai tukemaan kirjailijan luovuutta, mutta puheen tai tekstin piirteitä halutusti muokkaamalla myös matkimaan muita, vaarantamaan immateriaalioikeuksia tai tekemään petoksia. Koska tekoälyllä ei ole omaa tahtoa, pidemmän johdonmukaisesti etenevän tekstin tuottamiseksi tekoäly vaatii vielä ihmisen ohjausta.

Tekoälyllä generoitua kieltä voidaan käyttää henkilökohtaiseen opastukseen ja joukkojen ohjaukseen, mutta myös kaupalliseen tai poliittiseen manipulointiin ja provosointiin. Open AI:n GPT-3 -kielimallia käytetään jo yli 300 sovelluksessa ja se tuottaa lähes viisi miljardia sanaa päivässä. Tällaisen kyvykkyyden valjastaminen trollaamiseen voi vaikuttaa vahvasti yleiseen mielipiteeseen tai jopa tukkeuttaa sosiaalisen median ja estää muiden, kuten viranomaisviestien perillemenon. Kyseessä on selkeästi kansallisen informaatiopuolustuksen piiriin kuuluva uhka, jonka vastaisen puolustuskyvykkyyden rakentaminen on syytä ottaa vakavasti yhteiskunnan resilienssin turvaamiseksi.

Tukiäly ja tietoisuus

Tekstianalyysi ja tekstin tuottaminen voidaan yhdistää keskustelevaksi tukiälyksi, joka voi sparrata opiskelijoita ja luovan työn tekijöitä kuten kirjailijoita sekä markkina-analyytikkoja, tuotekehittäjiä ja päätöksentekijöitä. Tällaisia lisätyn luovuuden työkaluja on jo markkinoilla. Ne eivät suinkaan korvaa ihmisen omaa luovuutta eivätkä poista päätöksentekijän vastuuta. Tutkimusten mukaan kaksi kolmasosaa tekoälyn antamista vastauksista sisältyy suoraan opetusdataan; ne on siis opittu ulkoa. Mallit jäljittelevät ihmisiä kaikessa, myös ennakkoluuloissa ja epätotuuksissa, korostaen näin datan laadun merkitystä. Koska tekoälyltä puuttuu yleinen arkijärki, massiiviset tekoälymallit ovat ihmisiä epätotuudellisimpia, ja rajatuissa aihepiireissä parhaaseen tulokseen päästäänkin pienemmillä räätälöidyillä malleilla, joiden selitettävyys on parempi.

Yleisen tekoälyn edellytyksenä ajatellaan olevan tietoisuuden kehittäminen tai sen kehittyminen itsestään. Ilmiö tunnetaan singulariteettina. Periaatteessa ihmiset kyvyt ylittävän itsetietoisen tekoälyn kehittymistä ei voi pitää mahdottomana, mutta yleisen käsityksen mukaan siitä huolestuminen on suuresti ennenaikaista. Todelliset uhat tulevat siitä, että ihminen käyttää tekoälyä epäeettisiin ja vahingollisiin tarkoituksiin, ja nämä uhat ovat keskuudessamme jo tänään. Vaikka paniikkiin ei olekaan aihetta, on syytä varustautua tulevaisuuteen muun muassa tutkimuksen ja koulutuksen keinoin.

Tekoäly muutosvoimana

Kieliteknologiaan perustuivat tekoälyratkaisut parantavat yleisesti tiedon saavutettavuutta, ymmärrettävyyttä ja hyödynnettävyyttä. Arvovapaa teknologia on vahvasti mahdollistava niin yksilön, yritysten, yhteiskunnan kuin ympäristönkin näkökulmasta.

Kielten asema

Kieliteknologia madaltaa oleellisesti kielimuuria parantaen kansallista ja kansainvälistä vuorovaikutusta, yhdenvertaisuutta ja yhteisöllisyyttä. Toisaalta teknologisen kehityksen yksipuolistuminen uhkaa kaventaa kielellis-kulttuurista diversiteettiä tukahduttaen luovuutta ja heikentäen inhimillistä innovaatiopotentiaalia.

Digitalisaation tehostuminen

Tietoon pohjautuvan päätöksenteon tehostuminen parantaa merkittävästi terveydenhuollon, oppimisen ja yhteiskunnallisten palvelujen laatua, saatavuutta ja tehokkuutta. Sovellusten yksilöllistyminen parantaa niiden tuloksia ja edistää yhdenvertaisuutta. Kielellinen tekoäly voi myös tukea kulttuuria, luovuutta, luontoarvoja, innovointia, kaupallista toimeliaisuutta ja yrittäjyyttä sekä hidastaa kaupungistumiskehitystä.

Kaupallinen ja yhteiskunnallinen vaikuttaminen tehostuu. Fragmentoituva markkina antaa tilaa yhä yksilöllisemmille palveluille ja pienemmille toimijoille. Toisaalta globaali alustatalous uhkaa monopolisoida sovellusten tuottamat taloudelliset hyödyt ja muodostaa merkittäviä ylikansallisia yhteiskunnallisia toimijoita valtioiden rinnalle.

Yksityisyys, väärinkäytökset, valvonta ja vaikuttaminen

Dataistuminen ja digitaalisten palvelujen yhdentyminen uhkaavat yksityisyyttä. Väärinkäytökset yleistyvät, monipuolistuvat ja tulevat vaikeammiksi havaita. Tekoäly mahdollistaa myös valvonnan lisääntymisen. Toisaalta tekoälyn mahdollistaa myös uusia ratkaisuja yksityisyyden, luottamuksen ja turvallisuuden parantamiseksi. Yritysten ja yhteiskunnallisten toimijoiden lisäksi myös yksityiset ihmiset alkavat käyttää tekoälyä vaikeasti ennakoitavin tavoin, mikä aiheuttaa tarvetta uudenlaiselle sääntelylle.

Yhteiskunnallinen ja kaupallinen vaikuttaminen sekoittuvat ja tehostuvat merkittävästi. Teknologisten resurssien epätasaisuus saattaa vaarantaa yhdenvertaisuutta, mutta toisaalta fyysisten rajoitteiden poistuminen vähentää taloudellista riippuvuutta ja mahdollistaa paremmin myös vähemmistöjen äänen kuulumisen. Myös valtiollinen vaikuttaminen lisääntyy kasvattaen merkittävästi kyber- ja informaatiopuolustuksen tarvetta. Yhteiskunnan resilienssi riippuu yhä enemmän kansalaisten yleisestä tieto- ja taitotasosta, yhteisöllisyyden tunteesta ja puolustustahdosta.

Viestit päättäjille ja kansalaisille

Huippuosaaminen ja yleissivistys

Tutkimus ja koulutus ovat avainkeino tekoälyvallankumouksessa pärjäämiseksi. Huippuosaamista tarvitaan kansallisen valinnanvapauden ja vaikutusmahdollisuuksien varmistamiseksi. Korkea yleissivistys parantaa elämänlaatua ja yhdenvertaisuutta sekä edesauttaa terveiden markkinoiden kehitystä, yhteiskuntarauhaa ja turvallisuutta. Monipuolista kielten osaamista, kulttuurista diversiteettiä ja pienten kielialueiden huomioon ottamista kannattaa tukea kansallisesti, EU-tasolla ja kansainvälisesti.

Sääntely vs. kilpailukyky

Tietoturvan, yksityisyyden, yhdenvertaisuuden ja tasa-arvon sekä yleisen luottamuksen turvaamiseksi tekoälyn käyttöä on tarpeen säännellä kansainvälisessä yhteistyössä. Innovaatiokilpailukyvyn tukemiseksi on pyrittävä tekoälyn teknologiariippumattomaan määrittelyyn, asettaen vaatimuksia käytetyn datan laadulle ja eettisesti hyväksyttävälle, kestävän kehityksen mukaiselle käyttötarkoitukselle. Teknologisten ratkaisujen yhteensopivuutta tulee edistää standardein ja avoimin rajapinnoin. Päätöksenteon vastuut on määritettävä etukäteen, ja datan luovutuksessa informoidun suostumuksen käytänteitä kehitettävä käyttäjälähtöisesti. Sääntelyssä tule ottaa huomioon kaupallisten ja yhteiskunnallisten toimijoiden lisäksi yksilöiden muuttuvat roolit.

Kokonaisturvallisuus

Tietoturva, tietosuoja, yksityisyys ja luottamus ovat avaintekijöitä myös kansainvälisessä vuorovaikutuksessa. Lisääntyvän ja monipuolistuvan informaatiovaikuttamisen myötä kasvavien sisäisten ja ulkoisten turvallisuusriskien ennakointi ja informaatiopuolustuskyvyn parantaminen nousevat kansallisen turvallisuuden eturiviin.