



Bryssel 19.2.2020
COM(2020) 65 final

VALKOINEN KIRJA

Tekoälystä – Eurooppalainen lähestymistapa huippuosaamiseen ja luottamukseen

Valkoinen kirja tekoälystä

Eurooppalainen lähestymistapa huippuosaamiseen ja luottamukseen

Tekoäly kehittyy nopeasti. Se muuttaa elämäämme parantamalla terveydenhuoltoa (esim. tarkentamalla diagnosointia ja mahdollistamalla tautien paremman ehkäisyn), tehostamalla maataloutta, edistämällä ilmastomuutoksen torjuntaa ja siihen mukautumista, parantamalla tuotantojärjestelmien tehokkuutta ennakoivan kunnossapidon avulla, parantamalla eurooppalaisten turvallisuutta sekä monilla muilla tavoilla, joita voimme vain kuvitella. Samaan aikaan tekoälyyn liittyy useita mahdollisia riskejä, kuten läpinäkymätön päätöksenteko, sukupuoleen perustuva tai muunlainen syrjintä, tunkeutuminen yksityiselämäämme tai sen käyttö rikollisiin tarkoituksiin.

Ankaran kansainvälisen kilpailun vallitessa tarvitaan vankkaa eurooppalaista lähestymistapaa, joka perustuu huhtikuussa 2018 esitettyyn eurooppalaiseen tekoälystrategiaan¹. Jotta voitaisiin tarttua tekoälyn tarjoamiin mahdollisuuksiin ja vastata sen aiheuttamiin haasteisiin, EU:n on toimittava yhtenäisesti ja määriteltävä eurooppalaisten arvojen pohjalta oma tapansa edistää tekoälyn kehittämistä ja käyttöönottoa.

Komissio on sitoutunut mahdollistamaan tieteelliset läpimurrot, säilyttämään EU:n teknologisen johtoaseman ja varmistamaan, että uudet teknologiat palvelevat kaikkia eurooppalaisia parantamalla heidän elämäänsä kuitenkin heidän oikeuksiaan kunnioittaen.

Komission puheenjohtaja Ursula von der Leyen ilmoitti poliittisissa suuntaviivoissaan² aikovansa esittää koordinoitua eurooppalaista lähestymistapaa tekoälyn inhimillisiin ja eettisiin vaikutuksiin sekä pohdintaa siitä, kuinka massadataa voidaan käyttää paremmin innovoinnin tueksi.

Komissio tukee sääntelyyn ja investointeihin suuntautunutta lähestymistapaa, jonka kahtalaisena tavoitteena on edistää tekoälyn käyttöönottoa ja puuttua tämän uuden teknologian tiettyihin käyttötarkoituksiin liittyviin riskeihin. Tämän valkoisen kirjan tarkoituksena on esittää toimintavaihtoehtoja näiden tavoitteiden saavuttamiseksi. Siinä ei käsitellä tekoälyn kehittämistä ja käyttöä sotilaallisiin tarkoituksiin. Komissio pyytää jäsenvaltioita, muita EU:n toimielimiä ja kaikkia sidosryhmiä, kuten teollisuutta, työmarkkinaosapuolia, kansalaisyhteiskunnan organisaatioita, tutkijoita, suurta yleisöä ja kaikkia asiasta kiinnostuneita osapuolia ottamaan kantaa jäljempänä esitettyihin vaihtoehtoihin ja osallistumaan komission tulevaan päätöksentekoon tällä alalla.

1. JOHDANTO

Kun digitaalitekniologiasta tulee entistä keskeisempi osa ihmisten elämän kaikkia osa-alueita, ihmisten olisi voitava luottaa siihen. Luotettavuus on myös ennakoedellytys sen käyttöönotolle. Tämä on mahdollisuus Euroopalle, koska se on vahvasti sitoutunut arvoihin ja oikeusvaltioperiaatteeseen ja sillä on todistetusti valmiudet tuottaa turvallisia, luotettavia ja sofistikoituneita tuotteita ja palveluja ilmailusta energiaan, autoihin ja lääkinnällisiin laitteisiin.

Euroopan nykyinen ja tuleva kestävä talouskasvu ja yhteiskunnallinen hyvinvointi perustuvat entistä enemmän datan tuottamaan lisäarvoon. Tekoäly on yksi datavetoisen talouden tärkeimmistä sovelluksista. Nykyään suurin osa datasta liittyy kuluttajiin ja sitä säilytetään ja käsitellään

¹ Tekoäly Euroopassa, COM/2018/237 final.

² https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf.

keskitetyssä pilvipohjaisessa infrastruktuurissa. Sitä vastoin suuri osa huomisen paljon runsaammasta datasta tulee teollisuudelta, yrityksiltä ja julkiselta sektorilta ja sitä säilytetään monenlaisissa järjestelmissä, kuten verkon reunassa toimivissa laskentalaiteissa. Tämä avaa uusia mahdollisuuksia Euroopalle, jolla on vahva asema digitalisoidussa teollisuudessa ja yritysten välisissä sovelluksissa mutta suhteellisen heikko asema kuluttaja-alustoissa.

Yksinkertaisesti sanottuna tekoäly on joukko teknologioita, joissa yhdistetään dataa, algoritmeja ja laskentatehoa. Laskentatehon kasvu ja datan saatavuuden lisääntyminen ovat näin ollen keskeisiä tekoälyn nykyisen noususuhdanteen liikkeellepanevia voimia. Eurooppa voi yhdistää teknologiset ja teolliset vahvuutensa laadukkaaseen digitaaliseen infrastruktuuriin ja perusarvoihinsa perustuvaan sääntelykehykseen **saavuttaakseen maailmanlaajuisen johtoaseman datavetoisen talouden ja sen sovellusten innovoinnissa**, kuten Euroopan datastrategiassa esitetään³. Tältä pohjalta se voi kehittää tekoälyekosysteemin, joka tuo teknologian hyödyt koko Euroopan yhteiskunnan ja talouden ulottuville:

- **kansalaiset** voivat saada uusia hyötyjä esimerkiksi paremmasta terveydenhuollosta, kestävämmistä kodinkoneista, turvallisemmista ja puhtaammista liikennejärjestelmistä ja paremmista julkisista palveluista;
- **yritykset** voivat kehittää esimerkiksi uuden sukupolven tuotteita ja palveluja aloilla, joilla Eurooppa on erityisen vahva (koneteollisuus, liikenne, kyberturvallisuus, maatalous, vihreä talous ja kiertotalous, terveydenhuolto ja korkean lisäarvon alat kuten muoti ja matkailu); ja
- **yleistä etua koskevissa palveluissa** voidaan esimerkiksi vähentää palvelujen tarjoamisesta (liikenne, koulutus, energia ja jätehuolto) aiheutuvia kustannuksia, parantaa tuotteiden kestävyttä⁴ ja antaa lainvalvontaviranomaisten käyttöön asianmukaiset välineet kansalaisten turvallisuuden varmistamiseksi⁵ tarjoamalla pitävät takeet heidän oikeuksiensa ja vapauksiensa kunnioittamisesta.

Kun otetaan huomioon tekoälyn mahdollisesti merkittävä vaikutus yhteiskuntaamme sekä tarve rakentaa luottamusta, on olennaisen tärkeää, että eurooppalainen tekoäly perustuu arvoihimme ja perusoikeuksiimme, kuten ihmisarvoon ja yksityisyyden suojelemiseen.

Tekoälyjärjestelmien vaikutuksia olisi tarkasteltava paitsi yksilön näkökulmasta myös koko yhteiskunnan näkökulmasta. Tekoälyjärjestelmien käytöllä voi olla merkittävä rooli kestävän kehityksen tavoitteiden saavuttamisessa ja demokraattisen prosessin ja sosiaalisten oikeuksien tukemisessa. Hiljattain ehdotetun Euroopan vihreän kehityksen ohjelman⁶ myötä Eurooppa on edelläkävijä ilmastoon ja ympäristöön liittyvien haasteiden ratkaisemisessa. Tekoälyn kaltaiset digitaali teknologiat ovat olennaisen tärkeitä mahdollistavia tekijöitä vihreän kehityksen ohjelman tavoitteiden saavuttamisen kannalta. Tekoälyn kasvavan merkityksen vuoksi tekoälyjärjestelmien ympäristövaikutukset on otettava asianmukaisesti huomioon koko niiden elinkaaren ajan ja koko toimitusketjussa. Tämä koskee esimerkiksi algoritmien koulutuksessa ja datan tallentamisessa käytettyjä resursseja.

³ COM(2020) 66 final.

⁴ Tekoäly ja digitalisaatio yleensä ovat ratkaisevan tärkeitä edellytyksiä Euroopan kunnianhimoisen vihreän kehityksen ohjelman toteuttamiselle. Tieto- ja viestintätekniikka-alan nykyisen ympäristöjalanjäljen arvioidaan kuitenkin olevan yli 2 prosenttia kaikista päästöistä. Tähän valkoiseen kirjaan liittyvässä Euroopan digitaalistrategiassa ehdotetaan vihreää digitaalista muutosta tukevia toimenpiteitä.

⁵ Tekoälyvälineiden avulla EU:n kansalaisia voidaan suojella paremmin rikoksilta ja terroriteoilta. Tällaiset välineet voisivat esimerkiksi auttaa tunnistamaan verkossa olevan terroristisen propagandan, havaitsemaan epäilyttäviä liiketoimia vaarallisten tuotteiden myynnissä ja paljastamaan vaarallisia piilotettuja esineitä tai laittomia aineita tai tuotteita. Niiden avulla voitaisiin myös tarjota apua kansalaisille hätätilanteissa ja auttaa ohjaamaan pelastustyöntekijöitä.

⁶ COM(2019) 640 final.

Tekoälyn alalla tarvitaan yhteinen eurooppalainen lähestymistapa, jotta voidaan saavuttaa riittävä mittakaava ja välttää sisämarkkinoiden pirstaloituminen. Kansallisten aloitteiden käyttöönotto uhkaa vaarantaa oikeusvarmuuden, heikentää kansalaisten luottamusta ja estää dynaamisen eurooppalaisen teollisuuden syntymisen.

Tässä valkoisessa kirjassa esitetään toimintavaihtoehtoja, jotka mahdollistavat tekoälyn luotettavan ja turvallisen kehittämisen Euroopassa kunnioittaen täysin EU:n kansalaisten arvoja ja oikeuksia. Valkoisen kirjan tärkeimmät osatekijät ovat seuraavat:

- Poliittinen kehys, jossa määritellään toimenpiteet toimien yhdenmukaistamiseksi Euroopan, jäsenvaltioiden ja alueiden tasolla. Kehyksen tavoitteena on mobilisoida yksityisen ja julkisen sektorin yhteistyön avulla resursseja **’huippuosaamisen ekosysteemin’** luomiseksi koko arvoketjussa tutkimuksesta ja innovoinnista alkaen sekä luoda oikeanlaisia kannustimia tekoälyn perustuvien ratkaisujen käyttöönoton nopeuttamiseksi, myös pienissä ja keskisuurissa yrityksissä (pk-yrityksissä).
- Euroopan tekoälyä koskevan tulevan sääntelykehysten keskeiset osat, joilla luodaan ainutlaatuinen **’luottamuksen ekosysteemi’**. Tämän toteuttamiseksi kehyksessä on varmistettava EU:n sääntöjen noudattaminen, mukaan lukien perusoikeuksien ja kuluttajien oikeuksien suojelemista koskevat säännöt, etenkin sellaisissa EU:ssa toimivissa tekoälyjärjestelmissä, jotka aiheuttavat suuren riskin⁷. Luottamuksen ekosysteemin rakentaminen on poliittinen tavoite itsessään, ja sen pitäisi antaa kansalaisille luottamusta tekoälysovellusten käyttöönottoon ja tarjota yrityksille ja julkisille organisaatioille oikeusvarmuus innovoida tekoälyä käyttäen. Komissio tukee voimakkaasti ihmiskeskeistä lähestymistapaa, joka perustuu tiedonantoon luottamuksen rakentamisesta ihmiskeskeiseen tekoälyn⁸, ja se ottaa huomioon myös tekoälyä käsittelevän korkean tason asiantuntijaryhmän laatimien eettisten ohjeiden pilottivaiheessa saadun palautteen.

Tähän valkoiseen kirjaan liittyvällä Euroopan datastrategialla pyritään siihen, että Euroopasta voi tulla maailman houkuttelevin, turvallisin ja dynaaminen datavetoinen talous, joka voi käyttää dataa päätöksenteon ja kaikkien kansalaistensa elämän parantamiseksi. Strategiassa esitetään useita poliittisia toimenpiteitä, joita tarvitaan tämän tavoitteen saavuttamiseksi, kuten yksityisten ja julkisten investointien mobilisointi. Lisäksi tähän valkoiseen kirjaan liittyvässä komission kertomuksessa analysoidaan tekoälyn, esineiden internetin ja muiden digitaaliteknologioiden vaikutuksia turvallisuutta ja vastuuta koskevaan lainsäädäntöön.

2. TEOLLISTEN JA AMMATILLISTEN MARKKINOIDEN VAHVUUKSIEN HYÖDYNTÄMINEN

Euroopalla on hyvät mahdollisuudet hyödyntää tekoälyn tarjoamia mahdollisuuksia sekä käyttäjänä että tämän teknologian luoja ja tuottajana. Euroopassa on huippuluokan tutkimuskeskuksia ja innovatiivisia startup-yrityksiä. Sillä on johtava asema robotiikassa ja kilpailukykyiset valmistus- ja palvelusektorit autoteollisuudesta terveydenhuoltoon, energiasta rahoituspalveluihin ja maatalouteen. Eurooppa on kehittänyt vahvan laskentainfrastruktuurin (esim. suurtehotietokoneet), jolla on olennainen merkitys tekoälyn toiminnalle. Euroopalla on myös hallussaan suuria määriä julkista ja teollista dataa, jonka potentiaalia ei tällä hetkellä hyödynnetä täydessä mitassa. Sillä on hyvin tunnustettuja teollisia vahvuuksia turvallisissa ja varmoissa digitaalisissa järjestelmissä, joiden

⁷ Rikollisissa tarkoituksissa tehtävän tekoälyn väärinkäytön ehkäisemiseksi ja torjumiseksi voi olla tarpeen ottaa käyttöön lisäjärjestelyjä, mutta se ei kuulu tämän valkoisen kirjan soveltamisalaan.

⁸ COM (2019) 168.

virrankulutus on vähäinen. Nämä järjestelmät ovat olennaisen tärkeitä tekoälyn jatkokehityksen kannalta.

Hyödyntämällä EU:n kapasiteettia investoida seuraavan sukupolven teknologioihin ja infrastruktuureihin sekä datalukutaidon kaltaisiin digikompetensseihin voidaan lisätä Euroopan teknologista riippumattomuutta datatalouden kannalta keskeisissä mahdollistavissa teknologioissa ja infrastruktuureissa. Infrastruktuurien olisi tuettava sellaisten eurooppalaisten datapoolien luomista, jotka mahdollistavat luotettavan tekoälyn eli tekoälyn, joka perustuu eurooppalaisiin arvoihin ja sääntöihin.

Euroopan olisi hyödynnettävä vahvuuksiaan vahvistaakseen asemaansa ekosysteemissä ja koko arvoketjussa tiettyjen laitteistojen valmistussektoreilta ohjelmistojen kautta aina palveluihin asti. Näin tapahtuu jo jossain määrin. Euroopassa tuotetaan yli neljännes kaikista teollisista ja ammatillisista palveluroboteista (esim. täsmäviljelyä, turvallisuuspalveluja, terveydenhuoltoa ja logistiikkaa varten), ja sillä on tärkeä rooli **yritysten ja organisaatioiden ohjelmistosovellusten** (yritysten väliset sovellukset, kuten toiminnanohjaus- ja suunnitteluohjelmistot) sekä sähköistä hallinnointia ja ”älykkäitä yrityksiä” tukevien sovellusten kehittämisessä ja käytössä.

Eurooppa on myös edelläkävijä tekoälyn käyttönotossa valmistusteollisuudessa. Yli puolet suurimmista valmistajista käyttää vähintään yhtä tekoälysovellusta valmistustoiminnassa⁹.

Yksi syy Euroopan vahvaan asemaan tutkimuksen alalla on EU:n rahoitusohjelma, joka on osoittautunut keskeiseksi tekijäksi toimien yhdistämisessä, päällekkäisyyksien välttämässä ja julkisten ja yksityisten investointien houkuttelemisessa jäsenvaltioissa. Kolmen viime vuoden aikana EU:n rahoitus tekoälyä koskevaan tutkimukseen ja innovointiin on kasvanut 1,5 miljardiin euroon, mikä merkitsee 70 prosentin kasvua edelliseen kauteen verrattuna.

Tutkimukseen ja innovointiin Euroopassa tehtävät investoinnit ovat kuitenkin edelleen vain murto-osa maailman muilla alueilla tehtävistä julkisista ja yksityisistä investoinneista. Tekoälyyn investoitiin Euroopassa noin 3,2 miljardia euroa vuonna 2016, kun Pohjois-Amerikassa investoitiin noin 12,1 miljardia euroa ja Aasiassa noin 6,5 miljardia euroa¹⁰. Vastatakseen tähän Euroopan on lisättävä investointejaan huomattavasti. Jäsenvaltioiden kanssa laadittu koordinoitu tekoälysuunnitelma¹¹ on osoittautumassa hyväksi lähtökohdaksi tekoälyä koskevan yhteistyön tiivistämisessä Euroopassa ja synergioiden luomisessa tekoälyn arvoketjuun tehtävien investointien maksimoimiseksi.

3. TULEVIEN MAHDOLLISUUKSIEN HYÖDYNTÄMINEN: SEURAAVA DATA-AALTO

Euroopalla on tällä hetkellä heikompi asema kuluttajasovelluksissa ja verkkoalustoissa, mikä johtaa epäedulliseen kilpailuasemaan datan saatavuudessa, mutta eri aloilla on tekeillä merkittäviä muutoksia datan arvossa ja uudelleenkäytössä. Maailmassa tuotetun datan määrä kasvaa nopeasti: vuonna 2018 dataa tuotettiin 33 tsettatavua (ZB), ja määrän odotetaan nousevan 175 tsettatavuun vuonna 2025¹². Jokainen uusi data-aalto avaa Euroopalle mahdollisuuksia vahvistaa jalansijaansa datavetoisessa taloudessa ja saavuttaa johtava asema maailmassa tällä alalla. Myös tapa, jolla dataa säilytetään ja käsitellään, muuttuu merkittävästi seuraavien viiden vuoden aikana. Nykyään 80 prosenttia pilvipalveluissa tehtävästä datan käsittelystä ja analysoinnista tapahtuu datakeskuksissa ja keskitetyissä laskentakeskustoissa ja 20 prosenttia älykkäissä verkkoon liitetyissä esineissä, kuten

⁹ Seuraavina tulevat Japani (30 %) ja Yhdysvallat (28 %). Lähde: CapGemini (2019).

¹⁰ 10 imperatives for Europe in the age of AI and automation, McKinsey, 2017.

¹¹ COM (2018) 795.

¹² IDC (2019).

autoissa, kodinkoneissa tai valmistusroboteissa, sekä lähellä käyttäjää sijaitsevilla tietojenkäsittelylaitteissa ("reunalaskenta"). Vuoteen 2025 mennessä nämä osuudet todennäköisesti muuttuvat merkittävästi¹³.

Euroopalla on maailmanlaajuinen johtoasema alhaisen virrankulutuksen elektroniikassa, joka on keskeisessä asemassa tekoälyssä tarvittavien seuraavan sukupolven erikoistuneiden prosessorien kannalta. Näitä markkinoita hallitsevat tällä hetkellä EU:n ulkopuoliset toimijat. Tilanne voisi muuttua sellaisten aloitteiden avulla kuten eurooppalainen prosessorialoite, jossa keskitytään vähän energiaa kuluttavien laskentajärjestelmien kehittämiseen sekä reunalaskentaa että seuraavan sukupolven suurteholaskentaa varten. Muutosta tukevat myös keskeisiä digitaali teknologioita käsittelevän yhteisyrityksen toimet. Yhteisyrityksen on määrä aloittaa toimintansa vuonna 2021. Eurooppa on johtavassa asemassa myös neuromorfisissa ratkaisuissa¹⁴, jotka soveltuvat ihanteellisesti teollisuusprosessien (teollisuus 4.0) ja liikennemuotojen automatisointiin. Ne voivat parantaa energiatehokkuutta useilla suuruusluokilla.

Kvanttilaskennan viimeaikainen kehitys johtaa käsittelykapasiteetin eksponentiaaliseen kasvuun¹⁵. Eurooppa voi olla tämän teknologian eturintamassa, koska sillä on tieteellisiä vahvuuksia kvanttilaskennassa ja koska Euroopan teollisuudella on vahva asema kvanttisimulaattoreissa ja kvanttilaskennan ohjelmointiympäristöissä. Kvanttitekniikan testaus- ja kokeilujärjestelyjen saatavuuden parantamiseen tähtäävät eurooppalaiset aloitteet auttavat soveltamaan näitä uusia kvanttiratkaisuja eri teollisuuden ja tutkimuksen aloilla.

Rinnakkain tämän kanssa Eurooppa johtaa edelleen tekoälyn algoritmisten perusteiden kehittämistä oman tieteellisen huipputaamansa pohjalta. On tarpeellista rakentaa siltoja tällä hetkellä erillään toimivien tutkimusalojen välille, kuten koneoppimisen ja syväoppimisen (jolle on ominaista rajallinen tulkittavuus, suuren datamäärän tarve mallien kouluttamiseksi ja korrelaatioiden avulla tapahtuva oppiminen) ja symbolisten lähestymistapojen (jossa säännöt luodaan ihmisen toimien avulla) välille. Symbolisen päättelyn yhdistäminen syviin hermoverkkoihin voi auttaa meitä parantamaan tekoälyn tulosten selitettävyyttä.

4. HUIPPUOSAAMISEN EKOSYSTEEMI

Jotta voitaisiin rakentaa huipputaamisen ekosysteemi, joka voi tukea tekoälyn kehittämistä ja käyttöönottoa EU:n talouden ja julkishallinnon kaikilla aloilla, toimia on tehostettava useilla eri tasoilla.

A. YHTEISTYÖ JÄSENVALTIOIDEN KANSSA

Huhtikuussa 2018 hyväksytyn tekoälystrategiansa¹⁶ mukaisesti komissio esitteli joulukuussa 2018 yhdessä jäsenvaltioiden kanssa laaditun koordinoitun suunnitelman, joka koskee tekoälyn kehittämistä ja käyttöä Euroopassa¹⁷.

Suunnitelmassa ehdotetaan noin 70:tä yhteistä tointia, joilla pyritään tiivistämään ja tehostamaan jäsenvaltioiden keskinäistä yhteistyötä ja niiden yhteistyötä komission kanssa keskeisillä aloilla, joita

¹³ Gartner (2017).

¹⁴ Neuromorfisilla ratkaisuilla tarkoitetaan mitä tahansa erittäin suuren mittakaavan integroitujen piirien järjestelmää, joka jäljittelee hermoston neurobiologisia rakenteita.

¹⁵ Kvanttitietokoneet pystyvät käsittelemään sekunneissa moninkertaisesti suurempia datajoukkoja kuin tämän päivän suorituskykyisimmät tietokoneet, mikä mahdollistaa uusien tekoälysovellusten kehittämisen eri aloilla.

¹⁶ [Tekoäly Euroopassa, COM\(2018\) 237](#).

¹⁷ [Koordinoitu tekoälysuunnitelma, COM\(2018\) 795](#).

ovat muun muassa tutkimus, investoinnit, markkinoille saattaminen, taidot ja osaaminen, data sekä kansainvälinen yhteistyö. Suunnitelman on määrä jatkua vuoteen 2027, ja sitä seurataan ja tarkistetaan säännöllisesti.

Tavoitteena on maksimoida tutkimukseen, innovointiin ja käyttöönottoon tehtävien investointien vaikutus, arvioida kansallisia tekoälystrategioita sekä hyödyntää ja laajentaa tekoälyä koskevaa koordinoitua suunnitelmaa jäsenvaltioiden kanssa.

- *Toimi 1: Komissio ehdottaa jäsenvaltioille koordinoitun suunnitelman tarkistamista vuoden 2020 loppuun mennessä ottaen huomioon valkoisesta kirjasta järjestetyn julkisen kuulemisen tulokset.*

Tekoälyyn osoitettavalla EU-tason rahoituksella olisi houkuteltava ja yhdistettävä investointeja aloilla, joilla tarvittavat toimet ylittävät sen, mitä yksittäinen jäsenvaltio voi saavuttaa. Tavoitteena on houkutella tekoälyyn vuosittain yli 20 miljardin euron¹⁸ kokonaisinvestoinnit EU:ssa seuraavan vuosikymmenen aikana. Yksityisten ja julkisten investointien houkuttelemiseksi EU asettaa saataville resursseja Digitaalinen Eurooppa -ohjelmasta ja Horisontti Eurooppa -ohjelmasta sekä Euroopan rakenne- ja investointirahastoista vähemmän kehittyneiden alueiden ja maaseutualueiden tarpeisiin vastaamiseksi.

Koordinoitussa suunnitelmassa voitaisiin käsitellä myös yhteiskunnallista ja ekologista hyvinvointia yhtenä tekoälyn keskeisenä periaatteena. Tekoälyjärjestelmät auttavat puuttumaan kaikkein polttavimpiin huolenaiheisiin, kuten ilmastonmuutokseen ja ympäristön tilan heikkenemiseen. On myös tärkeää, että tämä tapahtuu ympäristöystävällisellä tavalla. Tekoäly voi ja sen pitäisi itse tarkastella kriittisesti resurssien käyttöä ja energiankulutusta ja se olisi koulutettava tekemään ympäristön kannalta myönteisiä valintoja. Komissio harkitsee mahdollisuuksia kannustaa ja edistää näin toimivia tekoälyratkaisuja yhdessä jäsenvaltioiden kanssa.

B. TUTKIMUS- JA INNOVAATIOYHTEISÖN TOIMIEN KESKITTÄMINEN

Euroopalla ei ole varaa säilyttää nykyistä hajanaista osaamiskeskusten maisemaa, jossa yksikään keskus ei saavuta sellaista mittakaavaa, että se voisi kilpailla maailman johtavien tutkimuslaitosten kanssa. On välttämätöntä luoda enemmän synergioita ja verkostoja tekoälyn eurooppalaisten tutkimuskeskusten välille ja sovittaa yhteen niiden toimia huippuosaamisen parantamiseksi, parhaiden tutkijoiden säilyttämiseksi ja houkuttelemiseksi ja parhaan teknologian kehittämiseksi. Eurooppa tarvitsee tutkimuksen, innovoinnin ja asiantuntemuksen kärkikeskuksen, joka koordinoisi näitä toimia ja olisi tekoälyn huippuosaamisen esikuva maailmassa ja joka voi houkutella investointeja ja alan parhaita kykyjä.

Keskusten ja verkostojen olisi keskityttävä aloille, joilla Euroopalla on potentiaalia tulla maailmanlaajuisesti johtajaksi. Tällaisia aloja ovat teollisuus, terveydenhuolto, liikenne, rahoitusala, elintarvikkeiden arvoketjut, energia/ympäristö, metsätalous, maan havainnointi ja avaruus. Kaikilla näillä aloilla on käynnissä kilpailu maailmanlaajuisesta johtajuudesta, ja Euroopalla on huomattavaa potentiaalia, osaamista ja kokemusta¹⁹. Yhtä tärkeää on luoda testaus- ja kokeilupaikkoja, jotka tukevat uusien tekoälysovellusten kehittämistä ja myöhempää käyttöönottoa.

¹⁸ COM(2018) 237.

¹⁹ Tuleva Euroopan puolustusrahasto ja pysyvä rakenteellinen yhteistyö (PESCO) tarjoavat myös mahdollisuuksia tekoälyn tutkimukseen ja kehittämiseen. Nämä hankkeet olisi synkronoitava tekoälyä koskevien EU:n laajempien siviiliohjelmien kanssa.

- *Toimi 2: Komissio helpottaa sellaisten huippuosaamis- ja testauskeskusten perustamista, jotka voivat yhdistää eurooppalaisia, kansallisia ja yksityisiä investointeja, mahdollisesti myös uuden oikeudellisen välineen avulla. Komissio on osana vuosien 2021–2027 monivuotista rahoituskehystä ehdottanut Digitaalinen Eurooppa -ohjelmassa kunnianhimoista ja kohdennettua määrärahaa maailmanlaajuisten vertailutestauskeskusten tukemiseen Euroopassa. Sitä täydennetään tarvittaessa Horisontti Eurooppa -ohjelman tutkimus- ja innovointitoimilla.*

C. OSAAMINEN

Tekoälyä koskevaa eurooppalaista lähestymistapaa on tuettava keskittymällä voimakkaasti osaamiseen siinä esiintyvien vajeiden täyttämiseksi²⁰. Komissio esittää piakkoin vahvistetun osaamisohjelman, jolla pyritään varmistamaan, että kaikki eurooppalaiset voivat hyötyä EU:n talouden vihreästä ja digitaalisesta muutoksesta. Aloitteisiin voisi sisältyä myös alakohtaisten sääntelyviranomaisten tukeminen niiden tekoälytaitojen parantamiseksi, jotta asiaa koskevat säännöt voidaan panna täytäntöön tehokkaasti ja vaikuttavasti. Päivitetty digitaalisen koulutuksen toimintasuunnitelma auttaa hyödyntämään paremmin dataa ja tekoälypohjaista teknologiaa, kuten oppimisanalytiikkaa ja ennustavaa analytiikkaa, jotta voidaan parantaa koulutusjärjestelmiä ja tehdä niistä digitaaliaikaan sopivia. Suunnitelma myös lisää tekoälyä koskevaa tietoisuutta kaikilla koulutustasoilla, jotta voidaan lisätä kansalaisten valmiutta tehdä tietoon perustuvia päätöksiä, joihin tekoäly vaikuttaa yhä enemmän.

Tekoälyn kanssa työskentelyyn tarvittavien taitojen kehittäminen ja työvoiman osaamisen parantaminen siten, että ne soveltuvat tekoälyn perustuvaan muutokseen, tulee olemaan yksi painopistealue yhdessä jäsenvaltioiden kanssa laadittavassa tarkistetussa tekoälyä koskevassa koordinoitussa suunnitelmassa. Tähän voisi sisältyä eettisiin suuntaviivoihin sisältyvän arviointiluettelon muuttaminen tekoälyn kehittäjien alustavaksi ”opetussuunnitelmaksi”, joka asetetaan saataville resurssina koulutuslaitosten käyttöön. Erityisesti olisi pyrittävä lisäämään tällä alalla koulutettujen ja työskentelevien naisten määrää.

Eurooppalainen tekoälyn tutkimuksen ja innovoinnin kärkikeskus houkuttelisi lahjakkuuksia kaikkialta maailmasta sen tarjoamien mahdollisuuksien ansiosta. Se myös kehittäisi ja levittäisi huippuosaamista, joka voi saada jalansijaa ja kasvaa kaikkialla Euroopassa.

- *Toimi 3: Luodaan ja tuetaan Digitaalinen Eurooppa -ohjelman pitkälle viedyn osaamisen pilarin kautta johtavien yliopistojen ja korkeakoulujen verkostoja parhaiden professoreiden ja tutkijoiden houkuttelemiseksi ja maailman johtavien maisteriohjelmien tarjoamiseksi tekoälyn alalla.*

Osaamisen parantamisen lisäksi tekoälyjärjestelmien suunnittelu ja käyttö työpaikalla vaikuttaa suoraan työntekijöihin ja työnantajiin. Työmarkkinaosapuolten osallistuminen on ratkaisevan tärkeää, jotta voidaan varmistaa ihmiskeskeinen lähestymistapa tekoälyn työelämässä.

D. KESKIÖSSÄ PK-YRITYKSET

On myös tärkeää varmistaa, että pk-yritykset voivat saada ja käyttää tekoälyä. Tätä varten digitaali-innovaatiokeskittymiä²¹ ja tekoälyn tilausalustoja²² olisi vahvistettava edelleen ja niiden avulla olisi

²⁰ <https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu>

²¹ ec.europa.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.

edistettävä pk-yritysten välistä yhteistyötä. Digitaalinen Eurooppa -ohjelma on keskeinen väline tämän toteuttamiseksi. Kaikkien digitaali-innovaatiokeskittymien olisi tuettava pk-yrityksiä tekoälyn ymmärtämisessä ja käyttönotossa, mutta on tärkeää, että vähintään yksi innovaatiokeskittymä kussakin jäsenvaltiossa on pitkälle erikoistunut tekoölyyn.

Pk-yritysten ja startup-yritysten on voitava saada rahoitusta, jotta ne voivat mukauttaa prosessejaan tai innovoida tekoälyä käyttäen. Komissio aikoo tulevan tekoölyyn ja lohkoketjuun suunnatun 100 miljoonan euron pilotti-investointirahaston pohjalta parantaa edelleen rahoituksen saatavuutta tekoälyn alalla InvestEU-ohjelman puitteissa²³. Tekoäly mainitaan nimenomaisesti niiden alojen joukossa, joilla voidaan käyttää InvestEU-takuuta.

- *Toimi 4: Komissio tekee yhteistyötä jäsenvaltioiden kanssa sen varmistamiseksi, että vähintään yksi digitaali-innovaatiokeskittymä kussakin jäsenvaltiossa on pitkälle erikoistunut tekoölyyn. Digitaali-innovaatiokeskittymiä voidaan tukea Digitaalinen Eurooppa -ohjelmasta.*
- *Komissio ja Euroopan investointirahasto käynnistävät vuoden 2020 ensimmäisellä neljänneksellä 100 miljoonan euron pilottihankkeen, jossa annetaan oman pääoman ehtoista rahoitusta tekoälyn innovatiiviseen kehittämiseen. Komissio aikoo lisätä rahoitusta merkittävästi vuodesta 2021 alkaen InvestEU-ohjelman kautta edellyttäen, että monivuotisesta rahoituskehiksestä päästään lopulliseen sopimukseen.*

E. KUMPPANUUS YKSITYISEN SEKTORIN KANSSA

On myös tärkeää varmistaa, että yksityinen sektori osallistuu täysipainoisesti tutkimus- ja innovointiohjelman laatimiseen ja tarjoaa tarvittavan määrän yhteisinvestointeja. Tämä edellyttää laajapohjaisen julkisen ja yksityisen sektorin kumppanuuden perustamista ja yritysten ylimmän johdon sitoutumista.

- *Toimi 5: Komissio perustaa Horisontti Eurooppa -ohjelman puitteissa uuden julkisen ja yksityisen sektorin kumppanuuden tekoälyn, datan ja robotiikan alalla. Se yhdistää toimia, varmistaa tekoälyalan tutkimuksen ja innovoinnin koordinoinnin ja tekee yhteistyötä Horisontti Eurooppa -ohjelman muiden julkisen ja yksityisen sektorin kumppanuuksien sekä edellä mainittujen testauslaitosten ja digitaali-innovaatiokeskittymien kanssa.*

²² www.Ai4eu.eu.

²³ Europe.eu/investeu.

F. TEKÖÄLYN KÄYTTÖNOTON EDISTÄMINEN JULKISELLA SEKTORILLA

On tärkeää, että julkishallinnot, sairaalat, yleishyödylliset palvelut ja liikennepalvelut, finanssivalvojat sekä muut yleistä etua koskevat alat alkavat nopeasti ottamaan toiminnoissaan käyttöön tekoälyyn pohjautuvia tuotteita ja palveluja. Erityistä huomiota kiinnitetään terveydenhuoltoon ja liikenteeseen, koska näillä aloilla teknologia on kypsää laajamittaisen käyttöönottoon.

- *Toimi 6: Komissio käynnistää avoimia ja läpinäkyviä alakohtaisia vuoropuheluja, joissa asetetaan etusijalle terveydenhuolto, maaseutuhallinnot ja julkisten palvelujen tarjoajat. Tarkoituksena on esittää toimintasuunnitelma kehittämisen, kokeilun ja käyttöönoton helpottamiseksi. Alakohtaisten vuoropuhelujen pohjalta valmistellaan erityinen tekoälyn käyttöönottoa koskeva ohjelma, jolla tuetaan tekoälyjärjestelmien julkisia hankintoja ja autetaan muuttamaan itse julkisia hankintaprosesseja.*

G. DATAN JA LASKENTAINFRASTRUKTUURIN SAATAVUUDEN VARMISTAMINEN

Valkoisessa kirjassa esitetyt toiminta-alat täydentävät suunnitelmaa, joka esitetään samanaikaisesti Euroopan datastrategiassa. Datan saatavuuden ja hallinnan parantaminen on olennaisen tärkeää. Ilman dataa tekoälyn ja muiden digitaalisten sovellusten kehittäminen ei ole mahdollista. Valtava määrä vielä tuottamatta olevaa uutta dataa tarjoaa Euroopalle tilaisuuden asettautua data- ja tekoälymuutoksen etulinjaan. Edistämällä vastuullisia datanhallintakäytäntöjä ja FAIR-periaatteiden noudattamista datassa voidaan tukea luottamuksen rakentamista ja varmistaa datan uudelleenkäytettävyys²⁴. Yhtä tärkeää on investoida keskeisiin laskentateknologioihin ja -infrastruktuureihin.

Komissio on ehdottanut Digitaalinen Eurooppa -ohjelmassa yli 4 miljardin euron tukea suurteho- ja kvanttilaskentaan, mukaan lukien reunalaskenta sekä tekoäly-, data- ja pilvi-infrastruktuuri. Näitä painopisteitä käsitellään tarkemmin Euroopan datastrategiassa.

H. KANSAINVÄLISET NÄKÖKOHDAT

Euroopalla on hyvät mahdollisuudet toimia maailmanlaajuisesti johtavassa asemassa yhteisiin arvoihin perustuvien liittoutumien rakentamisessa ja tekoälyn eettisen käytön edistämisessä. Tekoälyä koskeva EU:n työ on jo vaikuttanut kansainvälisiin keskusteluihin. Kun korkean tason asiantuntijaryhmä laati eettisiä ohjeitaan, ryhmässä oli mukana joukko EU:n ulkopuolisia organisaatioita ja useita hallitusten tarkkailijoita. Samaan aikaan EU osallistui tiiviisti OECD:n tekoälyä koskevien eettisten periaatteiden laatimiseen²⁵. G20 hyväksyi sittemmin nämä periaatteet kesäkuussa 2019 antamassaan ministerien lausumassa kaupasta ja digitaalitaloudesta.

EU tunnustaa, että tekoälyä koskevaa tärkeää työtä tehdään myös monenvälisillä foorumeilla, kuten Euroopan neuvostossa, Yhdistyneiden kansakuntien kasvatus-, tiede- ja kulttuurijärjestössä (UNESCO), Taloudellisen yhteistyön ja kehityksen järjestössä (OECD), Maailman kauppajärjestössä ja Kansainvälisessä televiestintäliitossa (ITU). YK:ssa EU osallistuu digitaalista yhteistyötä käsittelevän korkean tason paneelin raportin jatkotoimiin, myös tekoälyä koskevien suositusten osalta.

EU jatkaa tekoälyyn liittyvää yhteistyötä samanmielisten maiden mutta myös maailmanlaajuisen toimijoiden kanssa EU:n sääntöihin ja arvoihin perustuvan lähestymistavan pohjalta (esim. ylöspäin

²⁴ Löydettävyys, saatavuus, yhteentoimivuus ja uudelleenkäytettävyys; ks. FAIR-periaatteiden mukaista dataa käsittelevän komission asiantuntijaryhmän loppuraportti ja toimintasuunnitelma, 2018, https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

²⁵ <https://www.oecd.org/going-digital/ai/principles/>

tapahtuvan sääntelyn lähentämisen tukeminen, keskeisten resurssien kuten datan saatavuus, tasapuolisten toimintaedellytysten luominen). Komissio seuraa tiiviisti kolmansien maiden politiikkaa, joilla rajoitetaan datavirtoja, ja puuttuu aiheettomiin rajoituksiin kahdenvälisissä kauppaneuvotteluissa ja Maailman kauppajärjestön puitteissa toteutettavilla toimilla. Komissio on vakuuttunut siitä, että tekoälykysymyksiin liittyvän kansainvälisen yhteistyön on perustuttava lähestymistapaan, joka edistää perusoikeuksien kunnioittamista, mukaan lukien ihmisarvo, moniarvoisuus, osallisuus, syrjimättömyys sekä yksityisyyden ja henkilötietojen suoja²⁶, ja pyrkii viemään arvojaan kaikkialle maailmaan²⁷. On myös selvää, että tekoälyn vastuullinen kehittäminen ja käyttö voi olla liikkeellepaneva voima kestävän kehityksen tavoitteiden saavuttamisessa ja Agenda 2030:n toteuttamisessa.

5. LUOTTAMUKSEN EKOSYSTEEMI: TEKÖÄLYN SÄÄNTELYKEHYS

Kuten mikä tahansa uusi teknologia, tekoäly tuo mukanaan sekä mahdollisuuksia että riskejä. Kansalaiset pelkäävät, etteivät he voi puolustaa oikeuksiaan ja turvallisuuttaan kohdatessaan algoritmiseen päätöksentekoon liittyviä informaation epäsymmetrioita. Yritykset taas ovat huolissaan oikeudellisesta epävarmuudesta. Tekoäly voi auttaa suojelemaan kansalaisten turvallisuutta ja antamaan heille mahdollisuuden nauttia perusoikeuksistaan, mutta kansalaiset ovat huolissaan myös siitä, että tekoälyllä voi olla tahattomia vaikutuksia tai sitä voidaan jopa käyttää vihamielisiin tarkoituksiin. Näihin huolenaiheisiin on puututtava. Investointien ja osaamisen puutteen lisäksi tärkein tekoälyn laajempaa käyttöönottoa haittaava tekijä on luottamuksen puute.

Tämän vuoksi komissio esitti 25. huhtikuuta 2018 tekoälystrategian²⁸, jossa käsitellään tutkimukseen, innovointiin ja tekoälyvalmiuksiin kaikkialla EU:ssa tehtävien investointien kasvattamisen ohella myös tekoälyn sosioekonomisia näkökohtia. Komissio sopi jäsenvaltioiden kanssa koordinoitusta suunnitelmasta²⁹, jolla yhdenmukaistetaan strategioita. Komissio perusti myös korkean tason asiantuntijaryhmän, joka julkaisi huhtikuussa 2019 luotettavaa tekoälyä koskevat ohjeet³⁰.

Komissio antoi tiedonannon³¹, jossa se suhtautui myönteisesti korkean tason asiantuntijaryhmän laatimissa ohjeissa määriteltyihin seitsemään keskeiseen vaatimukseen:

- Ihmisen toimijuus ja ihmisen suorittama valvonta
- Tekninen luotettavuus ja turvallisuus
- Yksityisyyden suoja ja datan hallinta
- Läpinäkyvyys
- Monimuotoisuus, syrjimättömyys ja oikeudenmukaisuus
- Yhteiskunnallinen ja ekologinen hyvinvointi
- Vastuuvellisuus.

Ohjeisiin sisältyy myös arviointiluettelo, jota yritykset voivat soveltaa käytännössä. Noin 350 organisaatiota testasi arviointiluetteloa vuoden 2019 jälkipuoliskolla ja antoi siitä palautetta. Korkean tason ryhmä tarkistaa parhaillaan ohjeitaan tämän palautteen pohjalta ja saattaa tämän työn päätöksen kesäkuuhun 2020 mennessä. Palauteprosessin keskeinen tulos on se, että vaikka monet vaatimukset on

²⁶ Komissio rahoittaa kumppanuusvälineestä 2,5 miljoonan euron hanketta, joka helpottaa yhteistyötä samanmielisten kumppanien kanssa. Tarkoituksena on edistää EU:n tekoälyä koskevia eettisiä ohjeita ja hyväksyä yhteisiä periaatteita ja toimintaa koskevia päätelmiä.

²⁷ Puheenjohtaja Von der Leyen, ”Kunnianhimoisempi unioni: Ohjelma Euroopalle”, s. 17.

²⁸ COM (2018) 237.

²⁹ COM (2018) 795.

³⁰ <https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top>

³¹ COM(2019) 168.

jo otettu huomioon nykyisissä oikeus- tai sääntelyjärjestelmissä, läpinäkyvyyttä, jäljitettävyyttä ja ihmisen suorittamaa valvontaa koskevia vaatimuksia ei ole nimenomaisesti käsitelty voimassa olevassa lainsäädännössä monilla talouden aloilla.

Näiden korkean tason asiantuntijaryhmän ei-sitovien ohjeiden lisäksi ja puheenjohtajan poliittisten suuntaviivojen mukaisesti selkeä eurooppalainen sääntelykehys lisäisi kuluttajien ja yritysten luottamusta tekoälyyn ja nopeuttaisi siten teknologian käyttöönottoa. Tällaisen sääntelykehysten olisi oltava johdonmukainen muiden sellaisten toimien kanssa, joilla edistetään Euroopan innovointikapasiteettia ja kilpailukykyä tällä alalla. Sen on myös varmistettava sosiaalisesti, taloudellisesti ja ympäristön kannalta optimaaliset tulokset sekä EU:n lainsäädännön, periaatteiden ja arvojen noudattaminen. Tämä on erityisen tärkeää aloilla, joilla kansalaisten oikeuksiin voi kohdistua eniten välittömiä vaikutuksia, esimerkiksi kun tekoälysovelluksia käytetään lainvalvonnassa ja oikeuslaitoksessa.

Tekoälyn kehittäjiin ja käyttöönottajiin sovelletaan jo nyt perusoikeuksista (esim. tietosuojaa, yksityisyys, syrjimättömyys), kuluttajansuojasta sekä tuoteturvallisuudesta ja tuotevastuusta annettua EU:n lainsäädäntöä. Kuluttajat odottavat samantasoista turvallisuutta ja oikeuksiensa kunnioittamista riippumatta siitä, käytetäänkö tuotteessa tai järjestelmässä tekoälyä vai ei. Eräät tekoälyn erityispiirteet (esim. läpinäkyvättömyys) voivat kuitenkin vaikeuttaa tämän lainsäädännön soveltamista ja täytäntöönpanoa. Tästä syystä on tarpeen tutkia, voidaanko voimassa olevalla lainsäädännöllä puuttua tekoälyn riskeihin ja voidaanko se panna tehokkaasti täytäntöön vai tarvitaanko lainsäädännön mukauttamista tai uutta lainsäädäntöä.

Koska tekoäly kehittyy nopeasti, sääntelykehyksessä on jätettävä tilaa tulevan kehityksen huomioon ottamiselle. Mahdolliset muutokset olisi rajoitettava selkeästi yksilöityihin ongelmiin, joihin on olemassa toteuttamiskelpoisia ratkaisuja.

Jäsenvaltiot huomauttavat, että yhteistä eurooppalaista kehystä ei tällä hetkellä ole. Saksan dataetiikkakomissio on kehottanut ottamaan käyttöön riskiperusteisen viisitasoisen sääntelyjärjestelmän, jossa vaarattomimpia tekoälyjärjestelmiä ei säänneltäisi lainkaan ja vaarallisimmat järjestelmät kiellettäisiin kokonaan. Tanskassa on juuri otettu käyttöön dataeettisen merkin prototyyppi. Malta taas on ottanut käyttöön tekoälyä koskevan vapaaehtoisen sertifiointijärjestelmän. Jos EU ei määrittele EU:n laajuista lähestymistapaa, on olemassa todellinen vaara, että sisämarkkinat pirstaloituvat, mikä vaarantaisi luottamusta, oikeusvarmuutta ja markkinoille pääsyä koskevat tavoitteet.

Luotettavaa tekoälyä koskeva vankka eurooppalainen sääntelykehys suojelee kaikkia Euroopan kansalaisia ja auttaa luomaan kitkattomat sisämarkkinat tekoälyn edelleen kehittämistä ja käyttöönottoa varten sekä vahvistamaan tekoälyn teollista perustaa Euroopassa.

A. ONGELMAN MÄÄRITTELY

Tekoäly voi tuottaa paljon hyötyjä muun muassa tekemällä tuotteista ja prosesseista turvallisempia, mutta se voi myös aiheuttaa vahinkoa. Nämä vahingot voivat olla sekä aineellisia (ihmisten turvallisuus ja terveys, myös ihmishenkien menetys, omaisuusvahingot) että aineettomia (yksityisyyden menetys, sananvapauden rajoitukset, ihmisarvo, syrjintä esimerkiksi työsaannissa) ja ne voivat liittyä monenlaisiin riskeihin. Sääntelykehyksessä olisi keskityttävä siihen, kuinka erilaisia mahdollisten vahinkojen riskejä pienennetään, erityisesti merkittävimpiä riskejä.

Tekoälyn käyttöön liittyvät suurimmat riskit koskevat perusoikeuksien suojelemiseksi tarkoitettujen sääntöjen soveltamista (mukaan lukien henkilötietojen ja yksityisyyden suoja ja syrjimättömyys) sekä turvallisuuteen³² ja vastuuseen liittyviä kysymyksiä.

Perusoikeuksiin kohdistuvat riskit, mukaan lukien henkilötietojen ja yksityisyyden suoja ja syrjimättömyys

Tekoälyn käyttö voi vaikuttaa arvoihin, joille EU perustuu, ja johtaa perusoikeuksien rikkomiseen³³. Tämä koskee oikeutta sananvapauteen, kokoontumisvapauteen, ihmisarvoon ja syrjimättömyyteen sukupuolen, rodun tai etnisen alkuperän, uskonnon tai vakaumuksen, vammaisuuden, iän tai seksuaalisen suuntautumisen perusteella, siten kuin näitä oikeuksia sovelletaan yksittäisillä aloilla, oikeutta henkilötietojen ja yksityisyyteen suojaan³⁴ ja oikeutta tehokkaisiin oikeussuojakeinoihin ja oikeudenmukaiseen oikeudenkäyntiin sekä kuluttajansuojaa. Nämä riskit voivat johtua virheistä tekoälyjärjestelmien yleisessä suunnittelussa (myös ihmisen suorittaman valvonnan osalta) tai datan käytöstä ilman mahdollisten vinoutumien korjaamista (esim. järjestelmä on koulutettu käyttämällä ainoastaan tai pääasiassa miehiltä saatuja tietoja, jolloin tulokset eivät ole optimaalisia suhteessa naisiin).

Tekoäly voi suorittaa monia toimintoja, jotka aikaisemmin onnistuivat vain ihmisiltä. Tämän seurauksena kansalaiset ja oikeushenkilöt joutuvat yhä useammin tekoälyjärjestelmien tekemien tai niiden avustuksella tehtyjen toimien ja päätösten kohteeksi. Niitä voi joskus olla vaikea ymmärtää ja tarvittaessa kyseenalaistaa tehokkaasti. Tekoäly lisää myös mahdollisuuksia seurata ja analysoida ihmisten päivittäisiä tottumuksia. On esimerkiksi olemassa riski, että valtion viranomaiset tai muut tahot käyttävät tekoälyä laajamittaiseen valvontaan tai työnantajat käyttävät sitä työntekijöidensä käyttäytymisen seurantaan EU:n tietosuojaja muiden sääntöjen vastaisesti. Tekoälyn avulla voidaan analysoida suuria määriä tietoja ja havaita niiden välisiä yhteyksiä, jolloin sitä voidaan käyttää myös henkilöitä koskevien tietojen jäljittämiseen ja anonymisoinnin poistamiseen. Tämä aiheuttaa uusia henkilötietojen suojaan liittyviä riskejä jopa sellaisten tietoaaineistojen osalta, jotka eivät itsessään sisällä henkilötietoja. Myös verkossa toimivat välittäjät käyttävät tekoälyä priorisoidakseen käyttäjille suunnattua tietoa ja toteuttaakseen sisällön moderointia. Tietojen käsittely, tapa, jolla sovellukset on suunniteltu, ja ihmisen väliintulon mahdollisuudet voivat vaikuttaa sananvapautta, henkilötietojen suoja ja yksityisyyttä koskeviin oikeuksiin ja poliittisiin vapauksiin.

³² Tähän sisältyvät kyberturvallisuutta koskevat kysymykset, kriittisissä infrastruktuureissa käytettäviä tekoälysovelluksia koskevat kysymykset sekä tekoälyn vahingollinen käyttö.

³³ Euroopan neuvoston tutkimus osoittaa, että tekoälyn käyttö voi vaikuttaa moniin perusoikeuksiin, <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

³⁴ Näitä riskejä käsitellään yleisessä tietosuojasetuksessa ja sähköisen viestinnän tietosuojadirektiivissä (uudesta sähköisen viestinnän tietosuojasetuksesta neuvotellaan parhaillaan), mutta saattaa olla tarpeen tutkia, aiheuttavatko tekoälyjärjestelmät lisäriskejä. Komissio seuraa ja arvioi jatkuvasti yleisen tietosuojasetuksen soveltamista.

Tiettyt tekoälyalgoritmit, joita käytetään rikosten uusimisen ennakoimiseen, näyttävät syrjivän sukupuolen ja rodun perusteella, sillä uusimisen todennäköisyys on erilainen naisilla miehiin verrattuna ja oman maan kansalaisilla ulkomaalaisiin verrattuna. *Lähde: Tolan S., Miron M., Gomez E. and Castillo C. "Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Best Paper Award, International Conference on AI and Law, 2019*

Tiettyt kasvojen analysointiin käytettävät tekoälyohjelmat näyttävät syrjivän sukupuolen ja rodun perusteella, sillä ne tuottavat vain vähän virheitä vaaleaihoisten miesten sukupuolen määrittelyssä, mutta paljon virheitä, kun määriteltävänä on tummaihoisten naisten sukupuoli. *Lähde: Joy Buolamwini, Timnit Gebru; Proceedings of the 1st Conference on Fairness, Accountability and Transparency, PMLR 81:77-91, 2018.*

Ennakkoluulot ja syrjintä ovat minkä tahansa yhteiskunnallisen tai taloudellisen toiminnan luontaisia riskejä. Inhimillinen päätöksenteko ei ole immuuni virheille ja ennakkoluuloille. Samanlaisella ennakkoluulolla voisi kuitenkin tekoälyyn yhdistettynä olla paljon suurempi vaikutus, ja ilman ihmisen käyttäytymistä sääteleviä sosiaalisen valvonnan mekanismeja se voisi syrjiä monia ihmisiä³⁵. Näin voi käydä myös silloin kun järjestelmä ”oppii” ollessaan toiminnassa. Tällaisissa tapauksissa, joissa tulosta ei olisi voitu estää tai ennakoida suunnitteluvaiheessa, riskit eivät johdu järjestelmän alkuperäisen suunnittelun virheestä vaan pikemminkin niiden korrelaatioiden tai mallien käytännön vaikutuksista, joita järjestelmä havaitsee laajoissa tietoaaineistossa.

Monien tekoälyteknologioiden erityispiirteet, kuten läpinäkyvättömyys (”musta laatikko” -vaikutus), monimutkaisuus, ennakoimattomuus ja osittain autonominen käyttäytyminen, voivat vaikeuttaa perusoikeuksien suojelemiseksi tarkoitettujen voimassa olevan EU:n lainsäädännön sääntöjen noudattamisen varmistamista ja haitata niiden tehokasta täytäntöönpanoa. Lainvalvontaviranomaisilla ja asianomaisilla henkilöillä ei ehkä ole keinoja varmentaa, kuinka tietty tekoälyn avustuksella tehty päätös on tehty ja onko asiaa koskevia sääntöjä noudatettu. Luonnollisilla henkilöillä ja oikeushenkilöillä voi olla vaikeuksia tehokkaan oikeussuojan saatavuudessa tilanteissa, joissa tällaiset päätökset voivat vaikuttaa heihin kielteisesti.

Turvallisuuteen ja vastuujärjestelmän tehokkaaseen toimintaan kohdistuvat riskit

Tekoälyteknologiat voivat aiheuttaa käyttäjille uusia turvallisuusriskejä, kun ne on sisällytetty tuotteisiin ja palveluihin. Esimerkiksi hahmontunnistustekniikan virheen tuloksena itseohjautuva auto voi tunnistaa väärin tiellä olevan esineen ja aiheuttaa onnettomuuden, josta aiheutuu henkilövahinkoja ja aineellisia vahinkoja. Perusoikeuksiin kohdistuvien riskien tavoin myös nämä riskit voivat johtua tekoälyteknologian suunnitteluvirheistä, datan saatavuuteen ja laatuun liittyvistä ongelmista tai muista koneoppimisesta johtuvista ongelmista. Jotkin näistä riskeistä eivät rajoitu tekoälyyn perustuviin tuotteisiin ja palveluihin, mutta tekoälyn käyttö voi lisätä tai pahentaa niitä.

³⁵ Komission miesten ja naisten yhtäläisiä mahdollisuuksia käsittelevä neuvoa-antava komitea laatii parhaillaan tekoälyä koskevaa lausuntoa, jossa analysoidaan muun muassa tekoälyn vaikutuksia sukupuolten tasa-arvoon. Komitean on määrä hyväksyä lausunto vuoden 2020 alkupuolella. Myös sukupuolten tasa-arvoa koskevassa EU:n strategiassa vuosille 2020–2024 käsitellään tekoälyn yhteyttä sukupuolten tasa-arvoon. Kansallisten tasa-arvoelinten eurooppalainen verkosto (Equinet) julkaisee raportin (laatijoina Robin Allen ja Dee Masters) otsikolla ”Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI”; raportti on määrä julkaista vuoden 2020 alussa.

Näitä riskejä koskevien selkeiden turvallisuussäännösten puuttuminen voi asianomaisille henkilöille aiheutuvien riskien lisäksi aiheuttaa oikeudellista epävarmuutta yrityksille, jotka markkinoivat tekoälyä käyttäviä tuotteitaan EU:ssa. Markkinavalvonta- ja lainvalvontaviranomaiset voivat joutua tilanteeseen, jossa niille on epäselvää, voivatko ne puuttua asiaan, koska niillä ei ehkä ole toimivaltuuksia ja/tai niillä ei ole asianmukaisia teknisiä valmiuksia järjestelmien tarkastamiseen³⁶. Oikeudellinen epävarmuus voi siten alentaa yleistä turvallisuustasoa ja heikentää eurooppalaisten yritysten kilpailukykyä.

Jos turvallisuusriskit toteutuvat, selkeiden vaatimusten puuttuminen ja edellä mainitut tekoälyteknologioiden erityispiirteet vaikeuttavat tekoälyjärjestelmien avulla tehtyjen mahdollisesti ongelmallisten päätösten jäljittämistä. Tämä voi puolestaan vaikeuttaa vahinkoa kärsineiden henkilöiden mahdollisuuksia saada korvauksia voimassa olevan EU:n ja kansallisen vastuulainsäädännön nojalla³⁷.

Tuotevastuudirektiivin mukaan valmistaja on vastuussa viallisen tuotteen aiheuttamista vahingoista. Itseohjautuvien autojen kaltaisten tekoälyn perustuvien järjestelmien tapauksessa voi kuitenkin olla vaikea todistaa tuotteen viallisuus, aiheutunut vahinko sekä näiden välinen syy-yhteys. On myös jonkin verran epävarmuutta sen suhteen, kuinka ja missä määrin tuotevastuudirektiiviä sovelletaan tiettyntyyppisiin vikoihin, esimerkiksi jos viat johtuvat tuotteen puutteellisesta kyberturvallisuudesta.

Edellä perusoikeuksien yhteydessä mainitut vaikeudet, jotka liittyvät tekoälyjärjestelmien tekemien mahdollisesti ongelmallisten päätösten jäljittämiseen, koskevat yhtälailla myös turvallisuuteen ja vastuuseen liittyviä kysymyksiä. Vahinkoa kärsineillä henkilöillä ei välttämättä ole tosiasiallista mahdollisuutta saada todisteita, joita tarvitaan asian ratkaisemiseksi tuomioistuimessa, ja heillä voi olla vähemmän tehokkaat oikeussuojamahdollisuudet kuin tilanteissa, joissa vahinko johtuu perinteisestä teknologiasta. Nämä riskit kasvavat tekoälyn käytön yleistyessä.

B. MAHDOLLISET MUKAUTUKSET TEKÖÄLYÄ KOSKEVAAN EU:N NYKYISEEN LAINSÄÄDÄNTÖKEHYKSEEN

EU:n mittava tuoteturvallisuus- ja tuotevastuulainsäädäntö³⁸, johon sisältyy alakohtaisia sääntöjä ja jota täydentää kansallinen lainsäädäntö, on merkityksellinen useiden uusien tekoälysovellusten kannalta ja mahdollisesti sovellettavissa niihin.

Perusoikeuksien ja kuluttajien oikeuksien suojelun osalta EU:n lainsäädäntökehykseen sisältyy muun muassa rotusyrjintädirektiivi³⁹, yhdenvertaista kohtelua työssä koskeva direktiivi⁴⁰, direktiivit miesten ja naisten yhdenvertaisesta kohtelusta työhön ja ammattiin liittyvissä asioissa sekä tavaroiden ja

³⁶ Esimerkkinä voidaan mainita lasten älykello. Tuote ei voi aiheuttaa välitöntä haittaa sitä käyttävälle lapselle, mutta riittävän turvallisuustason puuttuessa sitä voidaan helposti käyttää välineenä lapsen tavoittamiseksi. Markkinavalvontaviranomaisten voi olla vaikea puuttua tapauksiin, joissa riski ei liity tuotteeseen sinänsä.

³⁷ Tähän valkoiseen kirjaan liittyvässä komission kertomuksessa analysoidaan tekoälyn, esineiden internetin ja muiden digitaali-teknologioiden vaikutuksia turvallisuutta ja vastuuta koskevaan lainsäädäntöön.

³⁸ Tuoteturvallisuutta koskeva EU:n oikeudellinen kehys koostuu yleisestä tuoteturvallisuusedirektiivistä (direktiivi 2001/95/EY), joka muodostaa turvaverkon, ja lukuisista alakohtaisista säännöistä, jotka kattavat erilaisia tuoteryhmiä koneista, lentokoneista ja autoista leluihin ja lääkinnällisiin laitteisiin ja joilla pyritään varmistamaan terveyden ja turvallisuuden suojelun korkea taso. Tuotevastuuta koskevaa lainsäädäntöä täydennetään erilaisilla tuotteiden tai palvelujen aiheuttamia vahinkoja koskevilla siviilioikeudellisilla vastuujärjestelmillä.

³⁹ Direktiivi 2000/43/EY.

⁴⁰ Direktiivi 2000/78/EY.

palvelujen yhdenvertaisesta saatavuudesta⁴¹, lukuisia kuluttajansuojasääntöjä⁴² ja henkilötietojen ja yksityisyyden suojaa koskevia sääntöjä, erityisesti yleinen tietosuojasetus, sekä muuta alakohtaista lainsäädäntöä, joka kattaa henkilötietojen suojan, kuten direktiivi lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta⁴³. Lisäksi vuodesta 2025 alkaen sovelletaan tuotteiden ja palvelujen esteettömyysvaatimuksia koskevia sääntöjä, jotka on vahvistettu esteettömyyttä koskevassa eurooppalaisessa säädöksessä⁴⁴. Perusoikeuksia on kunnioitettava myös pantaessa täytäntöön muuta EU:n lainsäädäntöä esimerkiksi rahoituspalvelujen, maahanmuuton ja verkossa toimivien välittäjien vastuun alalla.

Vaikka EU:n lainsäädäntöä sovelletaan periaatteessa edelleen täysimääräisesti riippumatta siitä, käytetäänkö tekoälyä, on tärkeää arvioida, voidaanko sen täytäntöönpanoa valvoa riittävästi, jotta tekoälyjärjestelmien aiheuttamiin riskeihin voidaan puuttua, vai onko tiettyjä oikeudellisia välineitä tarpeellista mukauttaa.

Talouden toimijat ovat esimerkiksi edelleen täysin vastuussa siitä, että tekoäly on kuluttajia suojelevien nykyisten sääntöjen mukainen. Myöskään mikään kuluttajien käyttäytymisen algoritmien hyväksikäyttö voimassa olevien sääntöjen vastaisesti ei ole sallittua, ja rikkomuksista on rangaistava vastaavasti.

Komissio katsoo, että lainsäädäntökehystä voitaisiin parantaa seuraavien riskien ja tilanteiden huomioon ottamiseksi:

- *Voimassa olevan EU:n ja kansallisen lainsäädännön tehokas soveltaminen ja täytäntöönpano:* tekoälyn keskeiset piirteet luovat haasteita EU:n ja kansallisen lainsäädännön asianmukaisen soveltamisen ja täytäntöönpanon varmistamiselle. Puutteellinen läpinäkyvyys (tekoälyn läpinäkyvättömyys) vaikeuttaa lainsäädännön mahdollisten rikkomusten havaitsemista ja todistamista muun muassa sellaisten säännösten osalta, jotka koskevat perusoikeuksien suojelua, vastuuseen asettamista tai korvauksen vaatimisen edellytysten täyttymistä. Tehokkaan soveltamisen ja täytäntöönpanon varmistamiseksi voi siten olla tarpeen mukauttaa tai selkeyttää voimassa olevaa lainsäädäntöä tietyillä aloilla, muun muassa vastuuasioissa. Tätä kysymystä käsitellään tarkemmin tähän valkoiseen kirjaan liittyvässä kertomuksessa.
- *Voimassa olevan EU:n lainsäädännön riittämätön soveltamisala:* EU:n tuoteturvallisuuslainsäädännön keskeinen painopiste on tuotteiden markkinoille saattamisessa. EU:n tuoteturvallisuuslainsäädännön mukaan ohjelmiston, jos se on osa lopullista tuotetta, on oltava asiaankuuluvien tuoteturvallisuussääntöjen mukainen, mutta avoimena kysymyksenä on, kuuluuko erillinen ohjelmisto EU:n tuoteturvallisuuslainsäädännön soveltamisalaan – niiden tiettyjen alojen ulkopuolella, joilla sovelletaan nimenomaisia sääntöjä⁴⁵. Nykyisin voimassa olevaa EU:n yleistä turvallisuuslainsäädäntöä sovelletaan tuotteisiin mutta ei palveluihin eikä

⁴¹ Direktiivi 2004/113/EY; direktiivi 2006/54/EY.

⁴² Kuten sopimattomia kaupallisia menettelyjä koskeva direktiivi (direktiivi 2005/29/EY) ja kuluttajanoikeusdirektiivi (direktiivi 2011/83/EU).

⁴³ Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta.

⁴⁴ Direktiivi (EU) 2019/882 tuotteiden ja palvelujen esteettömyysvaatimuksista.

⁴⁵ Esimerkiksi ohjelmistoa, jonka valmistaja on tarkoittanut käytettäväksi lääkinnällisiin tarkoituksiin, pidetään lääkinnällisenä laitteena lääkinnällisiä laitteita koskevassa asetuksessa (asetus (EU) 2017/745).

siten periaatteessa myöskään tekoälyteknologiaan perustuviin palveluihin (esim. terveyspalvelut, rahoituspalvelut ja liikennepalvelut).

- *Tekoälyjärjestelmien muuttuva toiminnallisuus:* ohjelmistojen, myös tekoälyn, integrointi tuotteisiin voi muuttaa tällaisten tuotteiden ja järjestelmien toimintaa niiden elinkaaren aikana. Tämä koskee erityisesti järjestelmiä, jotka edellyttävät toistuvia ohjelmistopäivityksiä tai jotka perustuvat koneoppimiseen. Nämä ominaisuudet voivat aiheuttaa uusia riskejä, joita ei esiintynyt, kun järjestelmä saatettiin markkinoille. Näitä riskejä ei käsitellä riittävästi voimassa olevassa lainsäädännössä, jossa keskitytään pääasiassa markkinoille saattamisen hetkellä esiintyviin turvallisuusriskeihin.
- *Epävarmuus vastuun jakautumisesta toimitusketjun eri talouden toimijoiden välillä:* EU:n tuoteturvallisuuslainsäädännön mukaan vastuu kuuluu yleisesti ottaen markkinoille saatetun tuotteen valmistajalle. Tämä koskee kaikkia komponentteja, myös tekoälyjärjestelmiä. Säännöistä voi kuitenkin tulla epäselviä esimerkiksi silloin, kun tekoälyn lisää tuotteen markkinoille saattamisen jälkeen jokin muu osapuoli kuin valmistaja. Lisäksi EU:n tuotevastuulainsäädännössä säädetään valmistajien vastuusta, ja toimitusketjun muiden toimijoiden vastuu jätetään kansallisten vastuusääntöjen varaan.
- *Muutokset turvallisuuden käsitteessä:* tekoälyn käyttö tuotteissa ja palveluissa voi aiheuttaa riskejä, joita EU:n lainsäädännössä ei tällä hetkellä nimenomaisesti käsitellä. Nämä riskit voivat liittyä muun muassa kyberuhkiin, henkilökohtaiseen turvallisuuteen (liittyen esimerkiksi tekoälyn uusiin sovelluksiin kuten kodinkoneisiin) tai verkkoyhteyden menettämiseen. Näitä riskejä voi esiintyä, kun tuotteita saatetaan markkinoille, tai niitä voi seurata ohjelmistopäivityksistä tai itseoppimisesta, kun tuotetta käytetään. EU:n olisi hyödynnettävä täysimääräisesti käytettävissään olevia välineitä tekoälysovelluksiin liittyviä mahdollisia riskejä koskevan näyttöpohjan parantamiseksi, muun muassa käyttämällä EU:n kyberturvallisuusviraston (ENISA) kokemusta tekoälyn uhkaympäristön arvioinnissa.

Kuten edellä todettiin, useat jäsenvaltiot tutkivat jo vaihtoehtoja kansallisen lainsäädännön antamiseksi tekoälyn aiheuttamiin haasteisiin vastaamiseksi. Tästä aiheutuu sisämarkkinoiden pirstaloitumisen riski. Toisistaan poikkeavat kansalliset säännöt ovat omiaan luomaan esteitä yrityksille, jotka haluavat myydä ja käyttää tekoälyjärjestelmiä sisämarkkinoilla. Yhteisen lähestymistavan varmistaminen EU:n tasolla antaisi eurooppalaisille yrityksille mahdollisuuden hyötymään sujuvasta pääsystä sisämarkkinoille ja tukisi niiden kilpailukykyä maailmanmarkkinoilla.

Kertomus tekoälyn, esineiden internetin ja robotiikan vaikutuksista turvallisuuteen ja vastuuvollisuuteen

Kertomus on liitetty tähän valkoiseen kirjaan ja siinä analysoidaan asiaa koskevaa oikeudellista kehystä. Siinä yksilöidään tämän kehysten soveltamiseen liittyvät epävarmuustekijät, jotka johtuvat tekoälyn ja muiden digitaalitekniikoiden aiheuttamista erityisistä riskeistä.

Siinä todetaan, että nykyinen tuoteturvallisuuslainsäädäntö tukee jo laajennettua turvallisuuskäsitettä, joka suojaa kaikenlaisilta riskeiltä, joita tuotteesta aiheutuu sen käytön mukaan. Oikeusvarmuuden lisäämiseksi voitaisiin kuitenkin ottaa käyttöön säännöksiä, jotka nimenomaisesti kattavat kehittyvien digitaalitekniikoiden aiheuttamat uudet riskit.

- Tiettyjen tekoälyjärjestelmien autonominen käyttäytyminen niiden elinkaaren aikana voi aiheuttaa tuotteeseen merkittäviä turvallisuuteen vaikuttavia muutoksia, jotka voivat edellyttää uutta riskinarviointia. Lisäksi suojatoimenpiteenä saatetaan tarvita myös ihmisen suorittamaa valvontaa tuotesuunnittelusta alkaen tekoälytuotteiden ja -järjestelmien koko elinkaaren ajan.
- Valmistajille voitaisiin tarvittaessa asettaa nimenomaisia velvoitteita myös käyttäjien henkiseen turvallisuuteen kohdistuvien riskien osalta (esim. yhteistyö humanoidirobottien kanssa).
- Unionin tuoteturvallisuuslainsäädännössä voitaisiin asettaa erityisiä vaatimuksia, joilla puututaan virheellisestä datasta suunnitteluvaiheessa aiheutuviin turvallisuusriskeihin. Lisäksi voitaisiin säätää erityisvaatimuksia mekanismeille, joilla varmistetaan, että datan laatu säilyy koko tekoälytuotteiden ja -järjestelmien käytön ajan.
- Algoritmeihin perustuvien järjestelmien läpinäkyvyyteen voitaisiin puuttua läpinäkyvyysvaatimuksilla.
- Voimassa olevia sääntöjä on ehkä mukautettava ja selkeytettävä sellaisten erillisten ohjelmistojen osalta, jotka saatetaan markkinoille sellaisinaan tai jotka ladataan tuotteeseen sen markkinoille saattamisen jälkeen, kun niillä on vaikutusta turvallisuuteen.
- Koska toimitusketjut ovat uusien teknologioiden osalta entistä monimutkaisempia, oikeusvarmuutta voitaisiin lisätä säännöksillä, joissa nimenomaisesti edellytetään yhteistyötä toimitusketjun talouden toimijoiden ja käyttäjien välillä.

Tekoälyn, esineiden internetin ja robotiikan kaltaisten kehittyvien digitaalitekniikoiden ominaispiirteet voivat aiheuttaa haasteita vastuukehysten eri osatekijöille ja heikentää niiden tehokkuutta. Eräät näistä ominaispiirteistä voivat vaikeuttaa vahingon jäljittämistä henkilöön, mikä olisi tarpeen tuottamukseen perustuvan kanteen nostamiseksi useimpien kansallisten sääntöjen mukaisesti. Tämä voisi lisätä merkittävästi vahinkoa kärsineiden henkilöiden kustannuksia ja johtaa siihen, että korvausvaateita muita kuin valmistajia vastaan voi olla vaikea esittää tai näyttää toteen.

- Henkilöillä, jotka ovat kärsineet tekoälyjärjestelmien myötävaikutuksella aiheutunutta vahinkoa, on oltava saman tasoinen suoja kuin henkilöillä, jotka ovat kärsineet muiden teknologioiden aiheuttamasta vahinkoa, samalla kun teknologisten innovaatioiden olisi voitava kehittyä edelleen.
- Kaikkia vaihtoehtoja tämän tavoitteen saavuttamiseksi olisi arvioitava huolellisesti, mukaan lukien tuotevastuudirektiivin mahdolliset muutokset ja kansallisten vastuusääntöjen mahdollinen kohdennettu yhdenmukaistaminen. Komissio pyrkii esimerkiksi selvittämään, missä määrin monimutkaisuuden seurauksia voi mahdollisesti olla tarpeen lieventää mukauttamalla kansallisten vastuusääntöjen edellyttämää todistustaakkaa tekoälysovellusten toiminnasta aiheutuneiden vahinkojen tapauksessa.

Edellä esitetyn perusteella komissio päätelee, että voimassa olevaan lainsäädäntöön mahdollisesti tehtävien mukautusten lisäksi saatetaan tarvita uutta erityisesti tekoälyä koskevaa lainsäädäntöä, jotta EU:n oikeudellinen kehys olisi nykyiseen ja ennakoituun teknologiseen ja kaupalliseen kehitykseen soveltuva.

C. EU:N TULEVAN SÄÄNTELYKEHYKSEN SOVELTAMISALA

Tulevan tekoälyä koskevan erityisen sääntelykehysten keskeinen kysymys on sen soveltamisalan määrittely. Alustavana oletuksena on, että sääntelykehystä sovellettaisiin tekoälyyn perustuviin tuotteisiin ja palveluihin. Tekoäly olisi siksi määriteltävä selkeästi tässä valkoisessa kirjassa ja mahdollisissa tulevilla poliittisilla aloitteilla.

Komissio esitti tekoälyn ensimmäisen määritelmän tekoälyä Euroopassa koskevassa tiedonannossaan⁴⁶. Korkean tason asiantuntijaryhmä tarkensi tätä määritelmää edelleen⁴⁷.

Missä tahansa uudessa säädöksessä annettavan tekoälyn määritelmän on oltava riittävän joustava teknisen kehityksen huomioon ottamiseksi ja riittävän täsmällinen tarvittavan oikeusvarmuuden takaamiseksi.

Tätä valkoista kirjaa sekä kaikkia poliittisista aloitteista käytäviä tulevia keskusteluja varten vaikuttaa tärkeältä selventää tekoälyn keskeisiä osatekijöitä, jotka ovat ”data” ja ”algoritmit”. Tekoäly voidaan integroida laitteisiin. Koneoppimistekniikoiden tapauksessa, jotka muodostavat tekoälyn osa-alueen, algoritmit on koulutettu johtamaan data-aineiston pohjalta tiettyjä malleja, jotta voidaan määrittää tietyn tavoitteen

Esimerkiksi autonomisessa ajamisessa algoritmit käyttävät reaaliaikaisesti dataa, jota saadaan ajoneuvosta (nopeus, moottorin kulutus, iskunvaimentimet jne.) ja ajoneuvon koko ympäristöä skannaavista antureista (tie, liikennemerkkit, muut ajoneuvot, jalankulkijat jne.), ja päättävät, mihin suuntaan ja millä kiihtyvyydellä ja nopeudella ajoneuvon olisi kuljettava tietyn päämäärän saavuttamiseksi. Oppimalla havaitusta datasta algoritmit mukautuvat liikennetilanteeseen ja ulkoisiin olosuhteisiin, myös muiden kuljettajien käyttäytymiseen, ja päättävät mukavimman ja turvallisimman ajoreitin.

saavuttamiseksi tarvittavat toimet. Algoritmit voivat jatkaa oppimista, kun niitä käytetään. Tekoälypohjaiset tuotteet voivat toimia itsenäisesti havainnoimalla ympäristöään ja noudattamatta ennalta määrättyjä ohjeita, mutta niiden käyttäytyminen on suurelta osin niiden kehittäjien määrittelemää ja rajoittamaa. Ihmiset määrittävät ja ohjelmoivat tavoitteet, joihin tekoälyjärjestelmän olisi optimaalisesti pyrittävä.

EU:lla on käytössä tiukka oikeudellinen kehys, jolla muun muassa varmistetaan kuluttajansuoja, puututaan sopimattomiin kaupallisiin menettelyihin ja suojellaan henkilötietoja ja yksityisyyttä. EU:n säännöstö sisältää myös tiettyjä aloja (esim. terveydenhuolto, liikenne) koskevia erityissääntöjä. Näitä

⁴⁶ COM(2018) 237 final, s 1: ”Tekoäly on järjestelmä, joka pyrkii älykkäästi saavuttamaan asetettuja tavoitteita analysoimalla ympäristöään ja toimimalla osittain itsenäisesti. Tekoälyjärjestelmät voivat olla täysin ohjelmistopohjaisia ja toimia virtuaalimaailmassa (esimerkiksi äänikomennoilla ohjattavat digiapulaiset, kuva-analyysiohjelmistot, hakuohjelmistot, puheen- ja kasvojen tunnistusohjelmistot) tai laitteistojen osia (esimerkiksi edistyneet robotit, itsenäiset autot, nelikopterit (drone) tai esineiden internetin sovellukset).”

⁴⁷ Korkean tason asiantuntijaryhmä, Tekoälyn määritelmä, s. 8: ”Tekoälyjärjestelmät ovat ihmisten suunnitteleimia ohjelmistojärjestelmiä (ja mahdollisesti myös laitejärjestelmiä), jotka toimivat fyysisessä tai digitaalisessa ulottuvuudessa tietyn tavoitteen saavuttamiseksi havainnoimalla ympäristöään hankkimalla dataa, tulkitsemalla kerättyä jäsenneilyä tai jäsentämätöntä dataa, tekemällä päätelmiä tästä datasta johdetun tietämyksen pohjalta tai käsittelemällä tästä datasta johdettuja tietoja ja tekemällä päätöksiä parhaista toimista tavoitteen saavuttamiseksi. Tekoälyjärjestelmät voivat joko käyttää symbolisia sääntöjä tai oppia numeerisen mallin, ja ne voivat myös mukauttaa käyttäytymistään analysoimalla, kuinka niiden aiemmat toimet vaikuttavat ympäristöön.”

voimassa olevia EU:n lainsäädännön säännöksiä sovelletaan edelleen suhteessa tekoölyyn, vaikka tähän kehykseen voi olla tarpeen tehdä tiettyjä päivityksiä digitalisaation ja tekoölyn käytön huomioon ottamiseksi (ks. B jakso). Tämän seurauksena niitä näkökohtia, joita jo käsitellään voimassa olevassa horisontaalisessa tai alakohtaisessa lainsäädännössä (esim. lääkinnällisiä laitteita tai liikennejärjestelmiä koskevassa lainsäädännössä⁴⁸), säännellään jatkossakin tällä lainsäädännöllä.

Tekoölyä koskevan uuden sääntelykehyksen olisi oltava riittävän tehokas, jotta sen tavoitteet voidaan saavuttaa, mutta se ei kuitenkaan saisi olla liian määrävä siten, että se voisi aiheuttaa kohtuuttoman hallinnollisen rasitteen etenkin pk-yrityksille. Tämän tasapainon saavuttamiseksi komissio katsoo, että sen olisi noudatettava riskiperusteista lähestymistapaa.

Riskiperusteinen lähestymistapa on tärkeä sen varmistamiseksi, että sääntelytoimet ovat oikeasuhteisia. Se edellyttää kuitenkin selkeitä kriteerejä, joiden perusteella voidaan eriyttää erilaiset tekoölysovellukset, etenkin suhteessa siihen, ovatko ne ”suuririskisiä” vai eivät⁴⁹. Suuririskisen tekoölysovelluksen määrittelyn olisi oltava selkeä ja helposti kaikkien asianomaisten osapuolten ymmärrettävissä ja sovellettavissa. Vaikka tekoölysovellusta ei luokiteltaisikaan suuririskiseksi, siihen sovelletaan kuitenkin täysin jo olemassa olevia EU:n sääntöjä.

Komissio katsoo, että tiettyä tekoölysovellusta olisi yleisesti pidettävä suuririskisenä, jos sekä alaan että aiottuun käyttöön liittyy merkittäviä riskejä erityisesti turvallisuuden, kuluttajien oikeuksien ja perusoikeuksien suojelun kannalta. Tarkemmin sanottuna tekoölysovellus olisi katsottava suuririskiseksi, jos se täyttää seuraavat kaksi kumulatiivista kriteeriä:

- Ensinnäkin tekoölysovellusta käytetään alalla, jolla tyypillisesti toteutettujen toimintojen ominaispiirteet huomioon ottaen voidaan olettaa esiintyvän merkittäviä riskejä. Ensimmäisellä kriteerillä varmistetaan, että sääntelytoimet kohdistetaan alueille, joilla riskien katsotaan yleensä todennäköisimmin esiintyvän. Soveltamisalaan kuuluvat alat olisi lueteltava nimenomaisesti ja kattavasti uudessa sääntelykehyksessä. Tällaisia aloja ovat muun muassa terveydenhuolto, liikenne, energia ja osa julkista sektoria⁵⁰. Luetteloa olisi tarkasteltava uudelleen säännöllisesti ja tarvittaessa muutettava käytännön kehityksen perusteella.
- Toiseksi tekoölysovellusta käytetään kyseisellä alalla siten, että siitä syntyy todennäköisesti merkittäviä riskejä. Tässä toisessa kriteerissä tunnustetaan, että kaikkeen tekoölyn käyttöön valituilla aloilla ei välttämättä liity merkittäviä riskejä. Esimerkiksi vaikka terveydenhuolto voi yleensä olla merkityksellinen ala, sairaalan ajanvarausjärjestelmän vika ei tavallisesti aiheuta niin merkittäviä riskejä, että lainsäädäntötoimet olisivat perusteltuja. Tietyn käyttötarkoituksen riskitason arviointi voisi perustua asianomaisiin osapuoliin kohdistuvaan vaikutukseen. Esimerkkeinä voidaan mainita tekoölysovellusten käyttötarkoitukset, jotka aiheuttavat oikeudellisia tai vastaavalla tavalla merkittäviä vaikutuksia luonnollisen henkilön tai yrityksen oikeuksiin; jotka aiheuttavat loukkaantumisen, kuoleman tai merkittävän aineellisen tai aineettoman vahingon riskin; tai jotka aiheuttavat vaikutuksia, joita luonnolliset henkilöt tai oikeushenkilöt eivät voi kohtuudella välttää.

⁴⁸ Erilaisia turvallisuusnäkökohtia ja oikeudellisia vaikutuksia liittyy esimerkiksi tekoölyjärjestelmiin, jotka antavat erikoistunutta lääketieteellistä tietoa lääkäreille, tekoölyjärjestelmiin, jotka antavat lääketieteellistä tietoa suoraan potilaalle, ja tekoölyjärjestelmiin, jotka suorittavat itse lääketieteellisiä tehtäviä suoraan potilaalle. Komissio tutkii parhaillaan näitä terveydenhuollolle ominaisia turvallisuuteen ja vastuuseen liittyviä haasteita.

⁴⁹ EU:n lainsäädännössä ”riskit” voidaan luokitella eri tavalla kuin tässä kuvaillaan alasta riippuen, esimerkiksi tuoteturvallisuuden osalta.

⁵⁰ Julkiseen sektoriin voisivat kuulua esimerkiksi turvapaikka-asiat, maahanmuutto, rajavalvonta, oikeuslaitos, sosiaaliturva ja työvoimapolvelut.

Kahden kumulatiivisen kriteerin soveltaminen varmistaisi, että sääntelykehysten soveltamisala on kohdennettu, ja tarjoaisi oikeusvarmuuden. Uuteen sääntelykehykseen sisältyviä pakollisia vaatimuksia (ks. D jakso jäljempänä) sovellettaisiin periaatteessa vain sovelluksiin, jotka on määritelty suuririskisiksi näiden kahden kumulatiivisen kriteerin mukaisesti.

Edellä mainitusta riippumatta voi esiintyä myös poikkeustapauksia, joissa kyseessä olevien riskien luonteen vuoksi tekoälysovellusten käyttöä tiettyihin tarkoituksiin pidetään itsessään suuririskisenä, eli riippumatta kyseessä olevasta alasta, ja joissa jäljempänä esitettyjä vaatimuksia näin ollen sovellettaisiin edelleen⁵¹. Esimerkkeinä voidaan mainita erityisesti seuraavat:

- Tekoälysovellusten käyttöä työhönottoprosesseissa sekä tilanteissa, jotka vaikuttavat työntekijöiden oikeuksiin, pidettäisiin aina ”suuririskisenä”, kun otetaan huomioon tällaisen käytön merkitys yksilöille ja yhdenvertaista kohtelua työssä koskeva EU:n säännöstö, ja siksi jäljempänä esitettyjä vaatimuksia sovellettaisiin kaikissa tapauksissa. Huomioon voitaisiin ottaa myös muita kuluttajien oikeuksiin vaikuttavia erityissovelluksia.
- Tekoälysovellusten käyttöä biometriseen etätunnistukseen⁵² ja muihin yksityisyyteen puuttuviin valvontateknologioihin pidettäisiin aina ”suuririskisenä”, ja siksi jäljempänä esitettyjä vaatimuksia sovellettaisiin kaikissa tapauksissa.

D. VAATIMUSTYYPIT

Tekoälyä koskevaa tulevaa sääntelykehystä suunniteltaessa on tarpeen päättää siitä, minkä tyyppisiä pakollisia oikeudellisia vaatimuksia asianomaisille toimijoille asetetaan. Näitä vaatimuksia voidaan edelleen tarkentaa standardien avulla. Kuten edellä C jaksossa todetaan ja jo olemassa olevan lainsäädännön lisäksi, vaatimuksia sovellettaisiin ainoastaan suuririskisiin tekoälysovelluksiin, millä varmistetaan, että sääntelytoimet ovat kohdennettuja ja oikeasuhteisia.

Kun otetaan huomioon korkean tason asiantuntijaryhmän ohjeet ja edellä esitetyt seikat, suuririskisiä tekoälysovelluksia koskevat vaatimukset voisivat koostua seuraavista keskeisistä piirteistä, joita käsitellään tarkemmin jäljempänä:

- koulutusdata
- datan ja tietojen säilyttäminen
- tietojen antaminen
- varmuus ja tarkkuus
- ihmisen suorittama valvonta
- erityisvaatimukset tietyille tekoälysovelluksille, kuten biometriseen etätunnistukseen käytetyille sovelluksille.

Oikeusvarmuuden varmistamiseksi näitä vaatimuksia tarkennetaan edelleen, jotta voidaan tarjota selkeä viitekehys kaikille toimijoille, joiden on noudatettava niitä.

⁵¹ On tärkeää korostaa, että myös muita EU:n säädöksiä voidaan soveltaa. Tekoälysovellusten turvallisuuteen voidaan soveltaa esimerkiksi yleistä tuoteturvallisuutta koskevaa direktiiviä, kun tekoälysovellus on integroitu kulutushyödykkeeseen.

⁵² Biometrinen etätunnistus olisi erotettava biometrisestä todentamisesta (viimeksi mainittu on turvaprosessi, joka perustuu yksilön ainutlaatuisiin biologisiin ominaisuuksiin sen todentamiseksi, että henkilö on se joka hän väittää olevansa.) Biometrinen etätunnistaminen tarkoittaa sitä, että useiden henkilöiden henkilöllisyys määritetään biometristen tunnistajien (sormenjäljet, kasvokuva, iiris, verisuonikuviot jne.) avulla etäältä, julkisessa tilassa ja jatkuvalla tavalla vertaamalla niitä tietokantaan tallennettuihin tietoihin.

a) Koulutusdata

Nyt on tärkeämpää kuin koskaan edistää, vahvistaa ja puolustaa EU:n arvoja ja sääntöjä ja erityisesti EU:n lainsäädäntöön perustuvia kansalaisten oikeuksia. Nämä toimet ulottuvat epäilemättä myös tässä tarkasteltaviin suuririskisiin tekoälysovelluksiin, joita markkinoidaan ja käytetään EU:ssa.

Kuten edellä todetaan, tekoälyä ei ole ilman dataa. Monien tekoälyjärjestelmien toiminta sekä toimet ja päätökset, joihin ne voivat mahdollisesti johtaa, riippuvat suuresti siitä data-aineistosta, jolla järjestelmät on koulutettu. Olisi toteutettava tarvittavat toimenpiteet sen varmistamiseksi, että tekoälyjärjestelmien koulutuksessa käytettävän datan yhteydessä kunnioitetaan EU:n arvoja ja sääntöjä erityisesti turvallisuuden ja perusoikeuksien suojelua koskevien voimassa olevien säännösten osalta. Tekoälyjärjestelmien koulutuksessa käytettävien data-aineistojen osalta voitaisiin harkita seuraavia vaatimuksia:

- Vaatimukset, joilla pyritään antamaan kohtuulliset takeet siitä, että tekoälyjärjestelmän mahdollistamien tuotteiden tai palvelujen myöhempi käyttö on turvallista siinä mielessä, että se täyttää sovellettavissa EU:n turvallisuussäännöissä (olemassa olevissa ja mahdollisissa täydentävissä) asetetut vaatimukset. Esimerkiksi vaatimukset, joilla varmistetaan, että tekoälyjärjestelmät koulutetaan data-aineistoilla, jotka ovat riittävän laajoja ja kattavat kaikki asiaankuuluvat skenaariot vaarallisten tilanteiden välttämiseksi.
- Vaatimukset toteuttaa kohtuullisia toimenpiteitä, joilla pyritään varmistamaan, että tekoälyjärjestelmien myöhempi käyttö ei johda tuloksiin, joihin liittyy kiellettyä syrjintää. Näihin vaatimuksiin voisi sisältyä erityisesti velvoite käyttää data-aineistoja, jotka ovat riittävän edustavia erityisesti sen varmistamiseksi, että niissä otetaan asianmukaisesti huomioon kaikki sukupuoleen, etniseen alkuperään ja muihin mahdollisiin kiellettyihin syrjintäperusteisiin liittyvät merkitykselliset ulottuvuudet.
- Vaatimukset, joiden tarkoituksena on varmistaa, että yksityisyyden ja henkilötietojen suoja on riittävä tekoälyä hyödyntävien tuotteiden ja palvelujen käytön aikana. Yleisessä tietosuojasetuksessa ja lainvalvontatarkoituksessa käsiteltyjen henkilötietojen suojasta annetussa direktiivissä säännellään näitä näkökohtia kunkin säädöksen soveltamisalaan kuuluvissa asioissa.

b) Datan ja tietojen säilyttäminen

Kun otetaan huomioon sellaiset tekijät kuten monien tekoälyjärjestelmien monimutkaisuus ja läpinäkymättömyys sekä niihin liittyvät vaikeudet, joita saattaa esiintyä sovellettavien sääntöjen noudattamisen tehokkaassa todentamisessa ja täytäntöönpanossa, tarvitaan vaatimuksia, jotka koskevat algoritmin ohjelmointiin liittyvien tietojen ja suuririskisten tekoälyjärjestelmien kouluttamiseen käytettyä dataa koskevien tietojen säilyttämistä ja joissain tapauksissa itse datan säilyttämistä. Nämä vaatimukset mahdollistavat tekoälyjärjestelmien tekemien mahdollisesti ongelmallisten toimien tai päätösten jäljittämisen ja varmentamisen. Tämän ei pitäisi ainoastaan helpottaa valvontaa ja täytäntöönpanoa, vaan se voi myös kannustaa asianomaisia talouden toimijoita ottamaan varhaisessa vaiheessa huomioon tarpeen noudattaa näitä sääntöjä.

Tätä varten sääntelykehyksessä voitaisiin säätää, että seuraavat olisi säilytettävä:

- tarkat tiedot tekoälyjärjestelmien koulutuksessa ja testauksessa käytetyistä data-aineistoista, mukaan lukien kuvaus niiden pääpiirteistä ja siitä, kuinka data-aineisto on valittu;
- tietyissä perustelluissa tapauksissa itse data-aineistot;

- dokumentaatio tekoälyjärjestelmien rakentamisessa, testaamisessa ja validoinnissa käytetyistä ohjelmointi⁵³ - ja koulutusmenetelmistä, -prosesseista ja -tekniikoista, mukaan lukien tarvittaessa näkökohdat, joilla on merkitystä turvallisuuden ja kiellettyyn syrjintään johtavien vinoutumien välttämisen kannalta.

Tiedot, dokumentaatio ja tarvittaessa data-aineistot olisi säilytettävä rajoitetun ja kohtuullisen ajan, jotta voidaan varmistaa asiaa koskevan lainsäädännön tehokas täytäntöönpano. Olisi toteutettava toimenpiteitä sen varmistamiseksi, että ne ovat pyynnöstä saatavilla erityisesti toimivaltaisten viranomaisten suorittamaa testausta tai tarkastusta varten. Tarvittaessa olisi toteutettava järjestelyjä sen varmistamiseksi, että luottamukselliset tiedot, kuten liikesalaisuudet, suojataan.

c) Tietojen antaminen

Läpinäkyvyyttä tarvitaan myös edellä c alakohdassa mainittujen tietojen säilyttämistä koskevien vaatimusten lisäksi. Asetettujen tavoitteiden saavuttamiseksi – erityisesti tekoälyn vastuullisen käytön edistämiseksi, luottamuksen rakentamiseksi ja tarvittaessa oikeussuojakeinojen saannin helpottamiseksi – on tärkeää, että suuririskisten tekoälyjärjestelmien käytöstä annetaan ennakoivasti riittävästi tietoa.

Siksi voitaisiin harkita seuraavia vaatimuksia:

- Varmistetaan selkeiden tietojen antaminen tekoälyjärjestelmän kyvyistä ja rajoituksista, erityisesti järjestelmien suunnitellusta käyttötarkoituksesta, olosuhteista, joissa niiden voidaan olettaa toimivan tarkoitetulla tavalla, sekä odotetusta tarkkuustasosta määritellyn tarkoituksen saavuttamisessa. Nämä tiedot ovat tärkeitä erityisesti järjestelmien käyttöönottajille, mutta ne voivat olla merkityksellisiä myös toimivaltaisille viranomaisille ja asianomaisille osapuolille.
- Erillään tästä kansalaisille olisi tiedotettava selkeästi siitä, milloin he ovat vuorovaikutuksessa tekoälyjärjestelmän eivätkä ihmisen kanssa. EU:n tietosuojalainsäädäntöön sisältyy jo tiettyjä tämänkaltaisia sääntöjä⁵⁴, mutta lisävaatimukset voivat olla tarpeellisia edellä mainittujen tavoitteiden saavuttamiseksi. Tässä tapauksessa olisi vältettävä tarpeettomia rasitteita. Siksi tällaisia tietoja ei tarvitse antaa esimerkiksi tilanteissa, joissa kansalaisille on välittömästi selvää, että he ovat vuorovaikutuksessa tekoälyjärjestelmien kanssa. On myös tärkeää, että annetut tiedot ovat objektiivisia, tiiviitä ja helposti ymmärrettäviä. Tapa, jolla tiedot annetaan, olisi räätälöitävä kulloisenkin tilanteen mukaan.

d) Varmuus ja tarkkuus

Tekoälyjärjestelmien – ja etenkin suuririskisten tekoälysovellusten – on oltava teknisesti varmoja ja tarkkoja, jotta ne olisivat luotettavia. Tämä tarkoittaa, että tällaisia järjestelmiä on kehitettävä vastuullisella tavalla ja siten, että niiden mahdollisesti aiheuttamat riskit otetaan etukäteen asianmukaisesti huomioon. Niiden kehittämisen ja toiminnan on oltava sellaista, että varmistetaan tekoälyjärjestelmien luotettava käyttäytyminen suunnitellulla tavalla. Aiheutuvien vahinkojen riskin minimoimiseksi olisi toteutettava kaikki kohtuulliset toimenpiteet.

⁵³ Esimerkiksi algoritmia koskeva dokumentaatio, mukaan lukien se, mitä tarkoitusta varten malli on optimoitu, mitkä painot tietyille parametreille on suunniteltu alusta alkaen jne.

⁵⁴ Erityisesti yleisen tietosuoja-asetuksen 13 artiklan 2 kohdan f alakohdan mukaan rekisterinpitäjän on henkilötietoja saadessaan toimitettava rekisteröidylle automaattisen päätöksenteon olemassaoloa koskevat lisätiedot, jotka ovat tarpeen asianmukaisen ja läpinäkyvän käsittelyn takaamiseksi, sekä tiettyjä lisätietoja.

Siksi voitaisiin harkita seuraavia osatekijöitä:

- Vaatimukset, joilla varmistetaan, että tekoälyjärjestelmät ovat varmoja ja tarkkoja, tai ainakin vastaavat oikein tarkkuustasoaan elinkaaren kaikissa vaiheissa;
- Vaatimukset, joilla varmistetaan, että tulokset ovat toistettavissa;
- Vaatimukset, joilla varmistetaan, että tekoälyjärjestelmät voivat asianmukaisesti käsitellä virheitä tai epä johdonmukaisuuksia elinkaaren kaikissa vaiheissa.
- Vaatimukset, joilla varmistetaan, että tekoälyjärjestelmät kestävät sekä avoimia hyökkäyksiä että hienovaraisempia yrityksiä manipuloida dataa tai algoritmeja ja että tällaisissa tapauksissa toteutetaan lieventäviä toimenpiteitä.

e) Ihmisen suorittama valvonta

Ihmisen suorittama valvonta auttaa varmistamaan, ettei tekoälyjärjestelmä heikennä ihmisen itsenäistä päätäntävaltaa tai aiheuta muita kielteisiä vaikutuksia. Luotettavan, eettisen ja ihmiskeskeisen tekoälyn tavoite voidaan saavuttaa vain varmistamalla, että ihmiset osallistuvat asianmukaisesti suuririskisiin tekoälysovelluksiin.

Vaikka tekoälysovelluksia, joita tässä valkoisessa kirjassa on tarkasteltu erityistä oikeudellista järjestelmää varten, pidetään kaikkia suuririskisinä, ihmisen suorittaman valvonnan asianmukainen tyyppi ja taso voivat vaihdella tapauksesta toiseen. Se riippuu erityisesti järjestelmien aiotusta käytöstä sekä vaikutuksista, joita käytöllä voisi olla asianomaisiin kansalaisiin ja oikeushenkilöihin. Se ei myöskään rajoita yleisessä tietosuojasetuksessa vahvistettuja laillisia oikeuksia, kun tekoälyjärjestelmä käsittelee henkilötietoja. Ihmisen suorittamalla valvonnalla voisi olla esimerkiksi seuraavat ilmentymät:

- tekoälyjärjestelmän tulos ei tule voimaan, ellei ihminen ole aiemmin tarkistanut ja validoinut sitä (esim. sosiaaliturvaetuksia koskevan hakemuksen hylkäämisen voi tehdä vain ihminen);
- tekoälyjärjestelmän tulos tulee välittömästi voimaan, mutta ihmisen osallistuminen on varmistettu jälkikäteen (esim. luottokorttihakemuksen hylkäämisen voi käsitellä tekoälyjärjestelmä, mutta ihmisen on voitava tarkistaa se jälkikäteen);
- tekoälyjärjestelmän seuranta käytön aikana ja kyky puuttua sen toimintaan reaaliaikaisesti ja pysäyttää järjestelmä (esim. itseohjautuvassa autossa on pysäytyspainike tai -menetelmä, kun ihminen katsoo, ettei auto toimi turvallisesti);
- suunnitteluvaiheessa asettamalla tekoälyjärjestelmälle toiminnallisia rajoituksia (esim. itseohjautuvan auton on lopetettava toimintansa tietyissä huonon näkyvyyden olosuhteissa, kun anturit eivät välttämättä ole yhtä luotettavia, tai sen on kaikissa olosuhteissa säilytettävä määrätty etäisyys edellä olevaan ajoneuvoon).

f) Biometristä etätunnistusta koskevat erityisvaatimukset

Biometristen tietojen⁵⁵ kerääminen ja käyttö etätunnistusta⁵⁶ varten, esimerkiksi ottamalla käyttöön kasvontunnistus julkisissa tiloissa, aiheuttaa erityisiä riskejä perusoikeuksille⁵⁷. Tekoälyä hyödyntävien biometristen etätunnistusjärjestelmien käytön vaikutukset perusoikeuksiin voivat vaihdella huomattavasti käyttötarkoituksen, käyttöyhteyden ja käytön laajuuden mukaan.

EU:n tietosuojasäännöissä kielletään periaatteessa biometristen tietojen käsittely luonnollisen henkilön yksiselitteistä tunnistamista varten tiettyjä erityisolosuhteita lukuun ottamatta⁵⁸. Etenkin yleisen tietosuoja-asetuksen mukaan tällaiselle käsittelylle on vain rajallinen määrä perusteita, joista keskeinen on tärkeää yleistä etua koskevat syyt. Tässä tapauksessa käsittelyn on perustuttava unionin oikeuteen tai jäsenvaltion lainsäädäntöön, siihen on sovellettava oikeasuhtaisuutta koskevia vaatimuksia, siinä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä on sovellettava asianmukaisia suojatoimia. Lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta annetun direktiivin mukaan tällaisen käsittelyn on oltava ehdottoman välttämätöntä, sen on oltava periaatteessa sallittu unionin oikeudessa tai kansallisessa lainsäädännössä ja se edellyttää asianmukaisten suojatoimien toteuttamista. Koska kaikenlainen biometristen tietojen käsittely luonnollisen henkilön yksiselitteistä tunnistamista varten liittyy poikkeukseen unionin oikeudessa säädetystä kiellosta, siihen sovellettaisiin Euroopan unionin perusoikeuskirjaa.

EU:n nykyisten tietosuojasääntöjen ja perusoikeuskirjan mukaisesti tästä seuraa, että tekoälyä voidaan käyttää biometriseen etätunnistamiseen ainoastaan, jos tällainen käyttö on asianmukaisesti perusteltua ja oikeasuhteista ja siihen sovelletaan asianmukaisia suojatoimia.

Niiden mahdollisten yhteiskunnallisten huolenaiheiden huomioon ottamiseksi, jotka liittyvät tekoälyn käyttöön tällaisiin tarkoituksiin julkisissa tiloissa, ja sisämarkkinoiden pirstaloitumisen välttämiseksi komissio käynnistää laajan eurooppalaisen keskustelun erityisolosuhteista, jos sellaisia on, jotka voisivat oikeuttaa tällaisen käytön, sekä yhteisistä suojatoimista.

E. Osoitus

Siihen, kenelle edellä mainitut suuririskisiin tekoälysovelluksiin sovellettavat oikeudelliset vaatimukset on osoitettu, liittyy kaksi keskeistä kysymystä.

Ensinnäkin on pohdittava, kuinka velvoitteet on jaettava asianomaisten talouden toimijoiden kesken. Tekoälyjärjestelmän elinkaareen osallistuu monia toimijoita. Näihin lukeutuvat kehittäjä, käyttöönottaja (henkilö, joka käyttää tekoälyllä varustettua tuotetta tai palvelua) ja mahdollisesti muut

⁵⁵ Biometrisillä tiedoilla tarkoitetaan ”luonnollisen henkilön fyysisiin ja fysiologisiin ominaisuuksiin tai käyttäytymiseen liittyvällä teknisellä käsittelyllä saatuja henkilötietoja, kuten kasvokuvia tai sormenjälkitietoja, joiden perusteella kyseinen luonnollinen henkilö voidaan tunnistaa tai kyseisen henkilön tunnistaminen voidaan varmistaa.” (Lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta annetun direktiivin 3 artiklan 13 kohta; yleisen tietosuoja-asetuksen 4 artiklan 14 kohta; asetuksen (EU) 2018/1725 3 artiklan 18 kohta).

⁵⁶ Kasvontunnistuksen yhteydessä tunnistamisella tarkoitetaan sitä, että henkilön kasvokuvan mallia verrataan moniin muihin tietokantaan tallennettuihin malleihin sen selvittämiseksi, onko henkilön kuva tallennettu tietokantaan. Todentamista (tai varmentamista) puolestaan kutsutaan usein yksi yhteen -vastaavuudeksi (one-to-one matching). Sen avulla voidaan vertailla kahta biometristä mallia, joiden oletetaan yleensä kuuluvan samalle henkilölle. Kahta biometristä mallia verrataan sen määrittämiseksi, onko kahdessa kuvassa näkyvä henkilö sama. Menettelyä käytetään esimerkiksi lentoasemilla rajatarkastuksissa käytettävissä automaattisissa porteissa.

⁵⁷ Esimerkiksi ihmisarvolle. Samoin oikeus yksityiselämän kunnioittamiseen ja henkilötietojen suojaan ovat keskeisiä perusoikeuksia, jotka aiheuttavat huolta kasvojen tunnistusteknologian käytön yhteydessä. Vaikutuksia voi kohdistua myös erityisryhmien, kuten lasten, iäkkäiden ihmisten ja vammaisten, syrjimättömyyteen ja oikeuksiin. Teknologian käyttö ei saa myöskään heikentää sananvapautta ja yhdistymis- ja kokoontumisvapautta. Ks. Facial recognition technology: fundamental rights considerations in the context of law enforcement, <https://fra.europa.eu/en/publication/2019/facial-recognition>.

⁵⁸ Yleisen tietosuoja-asetuksen 9 artikla, lainvalvontatarkoituksessa käsiteltävien henkilötietojen suojasta annetun direktiivin 10 artikla. Ks. myös asetuksen (EU) 2018/1725 10 artikla (jota sovelletaan EU:n toimielimiin ja elimiin).

osapuolet (valmistaja, jakelija tai maahantuoja, palveluntarjoaja, ammattimainen tai yksityinen käyttäjä).

Komissio katsoo, että tulevassa sääntelykehyksessä kukin velvoite olisi osoitettava niille toimijoille, joilla on parhaat edellytykset puuttua mahdollisiin riskeihin. Esimerkiksi tekoälyn kehittäjillä voi olla parhaat mahdollisuudet puuttua kehittämisvaiheesta aiheutuviin riskeihin, mutta niiden kyky hallita riskejä käyttövaiheen aikana voi olla rajoitetumpi. Tässä tapauksessa asiaa koskeva velvoite olisi osoitettava käyttöönottajalle. Tämä ei vaikuta kysymykseen siitä, minkä osapuolen olisi oltava vastuussa mahdollisista vahingoista, jotta voidaan määritellä vastuu maksaa korvauksia loppukäyttäjille tai muille vahinkoa kärsineille osapuolille ja varmistaa oikeussuojan tehokas saatavuus. EU:n tuotevastuulainsäädännön mukaan valmistaja on vastuussa viallisista tuotteista, sanotun kuitenkin rajoittamatta sellaisten kansallisten lakien soveltamista, jotka voivat mahdollistaa korvauksen perimisen myös muilta osapuolilta.

Toiseksi herää kysymys lainsäädäntötoimen maantieteellisestä soveltamisalasta. Komission mielestä on ensiarvoisen tärkeää, että vaatimuksia sovelletaan kaikkiin asianomaisiin talouden toimijoihin, jotka tarjoavat tekoälyn mahdollistamia tuotteita tai palveluja EU:ssa, riippumatta siitä, ovatko ne sijoittautuneet EU:hun vai eivät. Muussa tapauksessa edellä mainittuja lainsäädäntötoimen tavoitteita ei voitaisi täysin saavuttaa.

F. SÄÄNNÖSTEN NOUDATTAMINEN JA TÄYTÄNTÖÖNPANO

Jotta voidaan varmistaa, että tekoäly on luotettavaa, turvallista ja eurooppalaisten arvojen ja sääntöjen mukaista, sovellettavia oikeudellisia vaatimuksia on noudatettava käytännössä ja sekä toimivaltaisten kansallisten ja eurooppalaisten viranomaisten että asianosaisten osapuolten on pantava ne tehokkaasti täytäntöön. Toimivaltaisten viranomaisten olisi voitava tutkia yksittäisiä tapauksia mutta myös arvioida vaikutuksia yhteiskuntaan.

Kun otetaan huomioon, että tietyt tekoälysovellukset aiheuttavat suuren riskin kansalaisille ja yhteiskunnalle (ks. A jakso edellä), komissio katsoo tässä vaiheessa, että vaatimustenmukaisuuden ennakkoarviointi olisi tarpeen sen tarkistamiseksi ja varmistamiseksi, että tietyt edellä mainittuja suuririskisiin sovelluksiin sovellettavia pakollisia vaatimuksia (ks. D jakso edellä) noudatetaan. Vaatimustenmukaisuuden ennakkoarviointiin voisi sisältyä testaus-, tarkastus- tai sertifiointimenettelyjä⁵⁹. Siihen voisi sisältyä kehitysvaiheessa käytettyjen algoritmien ja data-aineistojen tarkastuksia.

Suuririskisten tekoälysovellusten vaatimustenmukaisuuden arvioinnin olisi oltava osa vaatimustenmukaisuuden arviointimekanismeja, joita on jo olemassa lukuisille EU:n sisämarkkinoille saatettaville tuotteille. Jos tällaisiin olemassa oleviin mekanismeihin ei voida turvautua, voi olla tarpeen luoda vastaavia mekanismeja, joissa hyödynnetään parhaita käytäntöjä ja sidosryhmien ja eurooppalaisten standardointijärjestöjen mahdollista panosta. Kaikkien tällaisten uusien mekanismien olisi oltava oikeasuhteisia ja syrjimättömiä ja niissä olisi käytettävä läpinäkyviä ja puolueettomia kriteereitä kansainvälisten velvoitteiden mukaisesti.

Vaatimustenmukaisuuden ennakkoarviointeihin perustuvaa järjestelmää suunniteltaessa ja toteutettaessa olisi kiinnitettävä erityistä huomiota seuraaviin:

⁵⁹ Järjestelmä perustuisi EU:n vaatimustenmukaisuuden arviointimenettelyihin, katso päätös N:o 768/2008/EY tai asetus (EU) 2019/881 (kyberturvallisuusasetus), tekoälyn erityispiirteet huomioon ottaen. Ks. vuoden 2014 ”Sininen opas” EU:n tuotesääntöjen täytäntöönpanosta.

- Kaikkia edellä esitettyjä vaatimuksia ei ehkä voida todentaa vaatimustenmukaisuuden ennakoarvioinnilla. Esimerkiksi tietojen antamista koskeva vaatimus ei yleensä sovellu hyvin todennettavaksi tällaisen arvioinnin avulla.
- Erityisesti olisi otettava huomioon mahdollisuus, että tietyt tekoälyjärjestelmät voivat kehittyä ja oppia kokemuksista, mikä voi edellyttää toistuvia arviointeja kyseisten tekoälyjärjestelmien elinkaaren aikana.
- Tarve todentaa koulutuksessa käytetty data sekä tekoälyjärjestelmien rakentamisessa, testaamisessa ja validoinnissa käytetyt ohjelmointi- ja koulutusmenetelmät, -prosessit ja -tekniikat.
- Jos vaatimustenmukaisuuden arviointi osoittaa, että tekoälyjärjestelmä ei täytä vaatimuksia esimerkiksi sen kouluttamiseen käytettävän datan osalta, havaitut puutteet on korjattava esimerkiksi kouluttamalla järjestelmä uudelleen EU:ssa siten, että varmistetaan kaikkien sovellettavien vaatimusten täyttyminen.

Vaatimustenmukaisuuden arvoinnit olisivat pakollisia kaikille talouden toimijoille, joita vaatimukset koskevat, riippumatta niiden sijoittautumispaikasta⁶⁰. Pk-yritysten taakan rajoittamiseksi voitaisiin harkita jonkinlaista tukirakennetta muun muassa digitaali-innovaatiokeskittymien kautta. Myös standardit ja asiaa käsittelevät verkkotyökalut voisivat helpottaa vaatimusten noudattamista.

Vaatimustenmukaisuuden ennakoarvoinnit eivät saisi rajoittaa toimivaltaisten kansallisten viranomaisten suorittamaa säännösten noudattamisen seuranta ja jälkikäteishallintaa. Tämä pätee suuririskisiin tekoälysovelluksiin, mutta myös muihin lakisäätöiden vaatimusten soveltamisalaan kuuluviin tekoälysovelluksiin, vaikka yksittäiseen sovellukseen liittyvä suuri riski voi olla syynä siihen, että toimivaltaiset kansalliset viranomaiset kiinnittävät erityistä huomiota ensiksi mainittuihin. Jälkitarkastukset olisi mahdollistettava laatimalla riittävä dokumentaatio kyseessä olevasta tekoälysovelluksesta (ks. E jakso edellä), ja kolmansien osapuolten, kuten toimivaltaisten viranomaisten, olisi tarvittaessa voitava testata tällaisia sovelluksia. Tämä voi olla erityisen tärkeää silloin, kun on kyse perusoikeuksiin kohdistuvista riskeistä, jotka riippuvat asiayhteydestä. Tällaisen vaatimustenmukaisuuden valvonnan olisi oltava osa jatkuvaa markkinavalvontajärjestelmää. Hallinnointiin liittyviä näkökohtia käsitellään tarkemmin jäljempänä H jaksossa.

Lisäksi sekä suuririskisten että muiden tekoälysovellusten osalta olisi varmistettava tehokkaat oikeussuojakeinot osapuolille, joihin tekoälyjärjestelmät vaikuttavat kielteisesti. Vastuukysymyksiä käsitellään tarkemmin tähän valkoiseen kirjaan liitettyssä turvallisuus- ja vastuukehystä koskevassa kertomuksessa.

G. MUIDEN KUIN SUURIRISKISTEN TEKÖÄLYSOVELLUSTEN VAPAAEHTOINEN MERKINTÄ

Sellaisten tekoälysovellusten osalta, joita ei luokitella ”suuririskisiksi” (ks. C jakso edellä) ja joihin ei näin ollen sovelleta edellä kuvattuja pakollisia vaatimuksia (ks. D, E ja F jakso edellä), vaihtoehtona olisi sovellettavan lainsäädännön lisäksi ottaa käyttöön vapaaehtoinen merkintäjärjestelmä.

Tällaisessa järjestelmässä asianomaiset talouden toimijat, jotka eivät kuulu pakollisten vaatimusten piiriin, voisivat päättää soveltaa vapaaehtoisesti joko kyseisiä vaatimuksia tai tiettyjä vastaavia

⁶⁰ Ks. jäljempänä H jakso asiaa koskevasta hallintorakenteesta sekä elimistä, jotka on nimetty suorittamaan vaatimustenmukaisuuden arviointeja.

vaatimuksia, jotka on erityisesti vahvistettu vapaaehtoista järjestelmää varten. Asianomaisille talouden toimijoille myönnettäisiin laatumerkki niiden tekoälysovelluksia varten.

Vapaaehtoisen merkin avulla asianomaiset talouden toimijat voisivat osoittaa, että niiden tekoälypohjaiset tuotteet ja palvelut ovat luotettavia. Sen avulla käyttäjät voisivat helposti tunnistaa, että kyseiset tuotteet ja palvelut ovat tiettyjen objektiivisten ja standardoitujen EU:n laajuisten vertailuarvojen mukaisia ja ylittävät tavanomaisesti sovellettavat oikeudelliset velvoitteet. Tämä auttaisi lisäämään käyttäjien luottamusta tekoälyjärjestelmiin ja edistäisi teknologian yleistä käyttöönottoa.

Tämä vaihtoehto edellyttäisi uutta säädöstä, jossa vahvistetaan vapaaehtoisen merkinnän puitteet sellaisten tekoälyjärjestelmien kehittäjille ja/tai käyttöönottajille, joita ei pidetä suuririskisinä. Merkintäjärjestelmään osallistuminen olisi vapaaehtoista, mutta vaatimuksista tulisi sitovia sen jälkeen kun kehittäjä tai käyttöönottaja on valinnut merkin käytön. Ennako- ja jälkivalvonnan yhdistelmällä olisi varmistettava, että kaikkia vaatimuksia noudatetaan.

H. HALLINNOINTI

Kansallisten toimivaltaisten viranomaisten yhteistyökehyksen muodossa toteutettava tekoälyä koskeva eurooppalainen hallintorakenne on tarpeellinen, jotta voidaan välttää vastuiden hajaantuminen, parantaa valmiuksia jäsenvaltioissa ja varmistaa, että Euroopassa saadaan asteittain käyttöön tarvittavat valmiudet tekoälypohjaisten tuotteiden ja palvelujen testaukseen ja sertifiointiin. Tässä yhteydessä olisi hyödyllistä tukea toimivaltaisista kansallisista viranomaisista, jotta ne voivat täyttää tehtävänsä tekoälyä käytettäessä.

Eurooppalaisella hallintorakenteella voisi olla erilaisia tehtäviä: se voisi toimia foorumina säännölliselle tietojen ja parhaiden käytäntöjen vaihdolle ja tunnistaa uusia suuntauksia ja antaa neuvoja standardointitoiminnasta ja sertifiointista. Sillä olisi myös oltava keskeinen rooli oikeudellisen kehyksen täytäntöönpanon helpottamisessa esimerkiksi antamalla ohjeistusta ja lausuntoja ja tarjoamalla asiantuntemusta. Tätä varten sen olisi tukeuduttava kansallisten viranomaisten verkostoon sekä alakohtaisiin verkostoihin ja sääntelyviranomaisiin kansallisella ja EU:n tasolla. Lisäksi komissiota voisi avustaa asiantuntijakomitea.

Hallintorakenteen olisi taattava mahdollisimman suuri sidosryhmien osallistuminen. Sidosryhmiä – kuluttajajärjestöjä ja työmarkkinaosapuolia, yrityksiä, tutkijoita ja kansalaisjärjestöjä – olisi kuultava kehyksen täytäntöönpanosta ja kehittämisestä.

Kun otetaan huomioon jo olemassa olevat rakenteet esimerkiksi rahoituksen, lääkkeiden, ilmailun, lääkinnällisten laitteiden, kuluttajansuojan ja tietosuojan aloilla, hallintorakenteen ei pitäisi toistaa olemassa olevia tehtäviä. Sen sijaan sen olisi luotava tiiviit yhteydet muihin EU:n ja jäsenvaltioiden toimivaltaisiin viranomaisiin eri aloilla, jotta se voisi täydentää olemassa olevaa asiantuntemusta ja auttaa olemassa olevia viranomaisia seuraamaan ja valvomaan sellaista talouden toimijoiden toimintaa, johon liittyy tekoälyjärjestelmiä ja tekoälypohjaisia tuotteita ja palveluja.

Jos tätä vaihtoehtoa käytetään, vaatimustenmukaisuuden arviointi voitaisiin antaa jäsenvaltioiden nimeämien ilmoitettujen laitosten tehtäväksi. Testauskeskusten olisi mahdollistettava tekoälyjärjestelmien riippumaton auditointi ja arviointi edellä esitettyjen vaatimusten mukaisesti. Riippumaton arviointi lisää luottamusta ja varmistaa objektiivisuuden. Se voisi myös helpottaa asianomaisten toimivaltaisten viranomaisten työtä.

EU:lla on huipputason testaus- ja arviointikeskuksia, ja sen olisi kehitettävä kapasiteettiaan myös tekoälyn alalla. Kolmansiin maihin sijoittautuneet talouden toimijat, jotka haluavat päästä sisämarkkinoille, voisivat käyttää joko EU:hun sijoittautuneita nimettyjä elimiä tai tällaisen arvioinnin

suorittamiseen nimettyjä kolmansien maiden elimiä, jos kolmansien maiden kanssa on tehty vastavuoroista tunnustamista koskevat sopimukset.

Tekoölyyn liittyvä hallintorakenne ja tässä käsitellyt mahdolliset vaatimustenmukaisuuden arvioinnit jättäisivät voimassa olevan unionin lainsäädännön mukaiset asianomaisten toimivaltaisten viranomaisten valtuudet ja vastuut ennalleen tiettyjen alojen tai erityiskysymysten osalta (rahoitusala, lääkkeet, ilmasto, lääkinnälliset laitteet, kuluttajansuoja, tietosuoja jne.).

6. PÄÄTELMÄT

Tekoöly on strateginen teknologia, joka tarjoaa monia etuja kansalaisille, yrityksille ja koko yhteiskunnalle, kuitenkin sillä edellytyksellä, että se on ihmiskeskeistä, eettistä, kestävää ja perusoikeuksia ja -arvoja kunnioittavaa. Tekoöly tarjoaa merkittäviä tehokkuus- ja tuottavuushyötyjä, jotka voivat vahvistaa Euroopan teollisuuden kilpailukykyä ja parantaa kansalaisten hyvinvointia. Se voi myös auttaa löytämään ratkaisuja eräisiin polttavimpiin yhteiskunnallisiin haasteisiin, joita ovat muun muassa ilmastomuutoksen ja ympäristön pilaantumisen torjunta, kestävyys ja väestörakenteen muutoksiin liittyvät haasteet sekä demokratioidemme suojelu ja, kun se on tarpeellista ja oikeasuhtaista, rikollisuuden torjunta.

Jotta Eurooppa voisi hyödyntää täysimääräisesti tekoölyn tarjoamat mahdollisuudet, sen on kehitettävä ja vahvistettava tarvittavia teollisia ja teknologisia valmiuksia. Kuten tähän asiakirjaan liittyvässä Euroopan datastrategiassa esitetään, tämä edellyttää myös toimenpiteitä, joiden avulla EU:sta voi tulla maailmanlaajuinen datakeskittymä.

Tekoölyä koskevalla eurooppalaisella lähestymistavalla pyritään edistämään Euroopan innovointikapasiteettia tekoölyn alalla ja samalla tukemaan eettisen ja luotettavan tekoölyn kehittämistä ja käyttöönottoa koko EU:n taloudessa. Tekoölyn olisi toimittava ihmisten hyväksi ja oltava positiivinen voima yhteiskunnassa.

Komissio käynnistää tällä valkoisella kirjalla ja siihen liittyvällä turvallisuus- ja vastuukehystä koskevalla kertomuksella jäsenvaltioiden kansalaisyhteiskunnan, teollisuuden ja tiedeyhteisön laajan kuulemisen tekoölyä koskevaan eurooppalaiseen lähestymistapaan liittyvistä konkreettisista ehdotuksista. Näihin kuuluvat sekä poliittiset keinot, joilla pyritään lisäämään investointeja tutkimukseen ja innovointiin, parantamaan osaamisen kehittämistä ja tukemaan tekoölyn käyttöönottoa pk-yrityksissä, että tulevan sääntelykehityksen keskeisiä osatekijöitä koskevat ehdotukset. Kuuleminen mahdollistaa kaikkien asianomaisten osapuolten kanssa käytävän kattavan vuoropuhelun, jota hyödynnetään komission seuraavissa toimitissa.

Komissio pyytää kommentteja valkoisessa kirjassa esitetyistä ehdotuksista avoimella julkisella kuulemisella, joka on saatavilla osoitteessa https://ec.europa.eu/info/consultations_en. Kuulemisessa voi esittää kommentteja 19. toukokuuta 2020 saakka.

Vakiintuneen käytäntönsä mukaisesti komissio julkaisee julkisessa kuulemisessa saamansa kannanotot. On kuitenkin mahdollista pyytää, että kannanotot käsitellään kokonaan tai osittain luottamuksellisina. Tässä tapauksessa on selvästi merkittävä kannanoton etusivulle, että sitä ei saa julkaista, ja toimitettava komissiolle ei-luottamuksellinen versio julkaisemista varten.