EUROOPA
KOMISJON

Brüssel, 19.2.2020
COM(2020) 65 final

VALGE RAAMAT

Tehisintellekt:
Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast

Valge raamat tehisintellekti kohta: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast

Tehisintellekt areneb kiiresti. See muudab meie elu, tagades parema tervishoiu (näiteks suurendades diagnostika täpsust ja võimaldades paremini haigusi vältida), muutes põllumajandustegevuse tõhusamaks, aidates kliimamuutusi leevendada ja nendega kohaneda, tõhustades tänu ennetavale hooldusele tootmissüsteeme, suurendades Euroopa kodanike turvalisust ja veel tuhandel muul viisil, mida me ei oska ettegi kujutada. Samal ajal kaasneb tehisintellektiga terve hulk võimalikke riske, nagu otsustusprotsessi läbipaistmatus, sooline või muud liiki diskrimineerimine, inimeste privaatsuse rikkumine või tehisintellekti kasutamine kurjategijate poolt.

Üleilmses halastamatus konkurentsis on vaja kindlat Euroopa käsitust, mis tugineks 2018. aasta aprillis esitletud Euroopa tehisintellektistrateegiale[1]. EL peab tehisintellektiga seotud võimalustele ja probleemidele vastu minnes ühte jalga astuma ning ise otsustama, kuidas edendada tehisintellekti arendamist ja juurutamist, tuginedes Euroopa väärtustele.

Komisjoni kindel eesmärk on aidata kaasa teaduse murrangulistele edusammudele, säilitada ELi liidripositsioon tehnoloogia vallas ja tagada, et uus tehnoloogia teenib kõiki Euroopa kodanikke ja parandab nende elujärge ning et samal ajal austatakse nende õigusi.

Komisjoni president Ursula von der Leyen teatas oma poliitilistes suunistes,[2] et kavas on välja töötada kooskõlastatud Euroopa käsitus tehisintellekti inim- ja eetilisest mõjust ja algatada mõttetalgud, mille teema on suurandmete parem kasutamine innovatsiooni eesmärgil.

Seega toetab komisjon regulatsioonile ja investeeringutele suunatud lähenemisviisi, millel on kaks võrdset eesmärki: soodustada tehisintellekti kasutuselevõttu ja tegeleda selle uue tehnoloogia teatavate kasutusviisidega seotud riskidega. Käesoleva valge raamatu eesmärk on visandada poliitikavariandid, mille abil need eesmärgid saavutada. Selles ei käsitleta tehisintellekti arendamist ja kasutamist sõjalistel eesmärkidel. Komisjon kutsub üles liikmesriike, teisi Euroopa Liidu institutsioone ja kõiki sidusrühmi – nagu ettevõtjad, sotsiaalpartnerid, kodanikuühiskonna organisatsioonid, teadlased, laiem avalikkus ja kõik asjast huvitatud isikud –, et nad esitaksid oma kommentaarid allpool toodud variantidele ja annaksid oma panuse komisjoni tulevastesse otsustesse selles valdkonnas.

1. SISSEJUHATUS

Et digitehnoloogiast saab iga päevaga inimeste igapäevaelu kõigi tahkude üha olulisem osa, peaksid inimesed saama seda usaldada. Usaldusväärsus on ka üks selle kasutuselevõtu eeltingimusi. See on suurepärane võimalus Euroopa jaoks, kes on kindlalt pühendunud õigusriigi väärtustele ja põhimõtetele ning igati tõestanud, et ta suudab luua turvalisi, usaldusväärseid ja keerukaid tooteid ja teenuseid lennundusest energeetikani, autodest meditsiiniseadmeteni.

Euroopa praegune ja tulevane kestlik majanduskasv ja ühiskondlik heaolu tuginevad üha enam andmete loodud väärtusele. Tehisintellekt on üks andmepõhise majanduse kõige olulisemaid väljundeid. Praegu on suurem osa andmetest seotud tarbijatega ning neid säilitatakse ja töödeldakse keskses pilvepõhises taristus. Seevastu suur osa tuleviku palju suuremast andmehulgast pärineb tööstus-, ettevõtlus- ja avalikust sektorist ning seda säilitatakse paljudes väga erinevates süsteemides,

[1] Tehisintellekt Euroopa huvides (COM/2018/237 final).

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

eelkõige võrgu servades toimivates andmetöötlusseadmetes. See loob uued võimalused Euroopale, kellel on tugev positsioon digitööstuse ja ettevõtjatevaheliste rakenduste valdkonnas, kuid suhteliselt nõrk positsioon tarbijaplatvormide alal.

Lihtsalt väljendudes ühendab tehisintellekt tehnoloogialiike, milles põimuvad andmed, algoritmid ja andmetöötlusvõimsus. Seega on tehisintellekti praeguse kasvuspurdi taga ennekõike andmete töötlemise alal tehtud edusammud ja nende üha suurem kättesaadavus. Euroopa saab ühendada oma tehnoloogia ja tööstuse alased tugevad küljed kõrgetasemelise digitaristu ja liidu põhiväärtustele tugineva õigusraamistikuga, **et tõusta maailmas andmepõhise majanduse ja selle rakenduste vallas innovatsiooniliidri positsioonile**, nagu on kavandatud Euroopa andmestrateegias[3]. Sellest lähtudes saab ta välja töötada tehisintellekti ökosüsteemi, mis tagab tehnoloogia hüved kogu Euroopa ühiskonnale ja majandusele.

- **Kodanike** jaoks tähendab see selliseid uusi hüvesid nagu paremad tervishoiuteenused, harvemini katkiminevad kodumasinad, turvalisemad ja puhtamad transpordisüsteemid ning paremad kommunaalteenused.
- **Ettevõtluse** areng saab hoogu näiteks seeläbi, et töötatakse välja uue põlvkonna tooted ja teenused valdkondades, kus Euroopa on tugev, nagu masinatööstus, transport, küberturvalisus, põllumajandus, rohe- ja ringmajandus, tervishoid ning sellised suure lisaväärtusega sektorid nagu mood ja turism.
- **Avaliku huvi pakkuvate** teenuste vallas võib näiteks tuua teenuste (transport, haridus, energiaga varustamine ja jäätmekäitlus) osutamise kulu vähenemise, toodete suurema kestlikkuse[4] ning selle, et õiguskaitseasutused saavad sobivad vahendid kodanike turvalisuse tagamiseks,[5] samas kui kodanike õiguste ja vabaduste kaitseks on ette nähtud piisavad tagatised.

Võttes arvesse tehisintellekti võimalikku suurt mõju ühiskonnale ja vajadust suurendada usaldust, on eluliselt tähtis, et Euroopa tehisintellekt tugineks liidu sellistele väärtustele ja põhiõigustele nagu inimväärikus ja privaatsuse kaitse.

Peale selle tuleks tehisintellektisüsteemide mõju arvesse võtta mitte ainult üksikisiku, vaid ka ühiskonna kui terviku seisukohast. Tehisintellektisüsteemide kasutamisel võib olla oluline roll kestliku arengu eesmärkide saavutamises ning demokraatlike protsesside ja sotsiaalõiguste toetamises. Euroopa on oma hiljutiste ettepanekutega Euroopa rohelise kokkuleppe kohta[6] eeskujuks kliimamuutuste ja keskkonnaprobleemidega võitlemise vallas. Rohelise kokkuleppe eesmärkide saavutamise eeltingimus on digitehnoloogia, näiteks tehisintellekt. Tehisintellekti üha suureneva tähtsusega arvestades tuleb kindlasti arvestada tehisintellektisüsteemide keskkonnamõju kogu nende elutsükli jooksul ja kogu tarneahela ulatuses, näiteks seoses ressursside kasutamisega algoritmide treenimiseks ja andmete säilitamiseks.

[3] COM(2020) 66 final.
[4] Tehisintellekt ja digiüleminek üldiselt on Euroopa rohelise kokkuleppe eesmärkide saavutamise pant. Teisalt moodustab info- ja kommunikatsioonitehnoloogiasektori keskkonnajalajälg hinnangute kohaselt üle 2 % üleilmsest heitest. Käesoleva valge raamatu juurde kuuluvas Euroopa digitaalarengu strateegias tehakse ettepanekud meetmete kohta, millega muuta digivaldkond keskkonnahoidlikkumaks.
[5] Tehisintellektivahenditega võib olla võimalik kaitsta ELi kodanikke paremini kuritegevuse ja terroriaktide eest. Näiteks võib sellistest vahenditest abi olla, et leida internetis leviv terroristlik propaganda, avastada kahtlased tehingud ohtlike toodetega, leida ohtlikud peidetud esemed või ebaseaduslikud ained või tooted, anda kodanikele hädaabi ja aidata tegutseda päästetöötajatel.
[6] COM(2019) 640 final.

Euroopa ühist käsitust tehisintellektist on vaja selleks, et saavutada piisav mastaap ja vältida ühtse turu killustatust. Riiklike algatuste puhul on oht, et kannatab õiguskindlus, väheneb kodanike usaldus ja pärsitud on dünaamilise tegevusvaldkonna teke Euroopas.

Käesolevas valges raamatus pakutakse välja poliitikavariandid, mis võimaldavad tehisintellekti usaldusväärset ja turvalist väljatöötamist Euroopas, austades täielikult ELi kodanike väärtusi ja õigusi. Käesoleva valge raamatu peamised elemendid on järgmised.

- Poliitikaraamistik, millega kehtestatakse meetmed Euroopa, riikliku ja piirkondliku tasandi jõupingutuste kooskõlastamiseks. Raamistiku eesmärk on kaasata era- ja avaliku sektori koostöös ressursse, et luua kogu väärtusahelat hõlmav **tipptaseme ökosüsteem**, mis algaks teadustegevusest ja innovatsioonist, ning luua õiged stiimulid, et kiirendada tehisintellektil põhinevate lahenduste kasutuselevõttu, sealhulgas väikeste ja keskmise suurusega ettevõtjate (VKE) hulgas.
- Euroopa tehisintellekti tulevase reguleeriva raamistiku kesksed elemendid, mis loovad ainulaadse **usaldusväärse ökosüsteemi.** Selleks peab raamistik tagama vastavuse ELi normidele, sealhulgas põhiõigusi ja tarbijate õigusi kaitsvatele sätetele, eriti mis puudutab selliseid ELis toimivaid tehisintellektisüsteeme, millega on seotud suur risk[7]. Usaldusväärse ökosüsteemi loomine on omaette poliitikaeesmärk, mis peaks andma kodanikele julguse hakata tehisintellektirakendusi kasutama ning tagama ettevõtetele ja avalik-õiguslikele organisatsioonidele tehisintellekti põhise innovatsiooni juures õiguskindluse. Komisjon toetab jõuliselt inimkeskset lähenemisviisi, mis tugineb teatisele „Usalduse loomine inimkeskse tehisintellekti vastu“, [8] ja võtab samuti arvesse tagasisidet, mis saadi tehisintellekti kõrgetasemelise eksperdirühma koostatud eetikasuuniste katseetapis.

Käesoleva valge raamatu juurde kuuluva Euroopa andmestrateegia eesmärk on teha Euroopast maailma kõige atraktiivsem, turvalisem ja dünaamilisem osava andmekasutusega (*data-agile*) majanduskeskkond, võimestades Euroopat andmete varal paremaid otsuseid tegema ja kõigi oma kodanike elujärge parandama. Strateegias on esitatud terve hulk poliitikameetmeid, muu hulgas seoses era- ja avaliku sektori investeeringute kaasamisega, mis on vajalikud selle eesmärgi saavutamiseks. Lisaks sellele on käesoleva valge raamatu juurde kuuluvas komisjoni aruandes analüüsitud tehisintellekti, asjade interneti ja muu digitehnoloogia tähendust ohutus- ja vastutusalaste õigusaktide seisukohast.

2. KASUTAME ÄRA TUGEVUSE TÖÖSTUS- JA ERIALATURGUDEL

Euroopal on suurepärane positsioon tehisintellektist kasusaamiseks mitte pelgalt selle tehnoloogia kasutaja, vaid ka looja ja tootjana. Tal on suurepärased teaduskeskused, uuenduslikud idufirmad, juhtpositsioon maailmas robootika alal ning konkurentsivõimeline tööstus- ja teenustesektor autotööstusest tervishoiuni, energeetikast finantsteenuste ja põllumajanduseni. Euroopa on välja arendanud tugeva andmetöötlustaristu – st kõrgjõudlusega andmetöötlusseadmed –, mis on tehisintellekti toimimise pant. Samuti on Euroopa käsutuses suur hulk avaliku ja tööstussektori teavet, mille potentsiaal on praegu alakasutatud. Liidu tööstuse üks laialdaselt tunnustatud tugevaid külgi on väikese voolutarbega ohutud ja turvalised digisüsteemid, mis on tehisintellekti edasiarendamiseks hädavajalikud.

[7] Ehkki tehisintellekti kuritegelikul eesmärgil kasutamise vältimiseks ja sellega võitlemiseks võib olla vaja täiendavaid meetmeid, jääb see käesoleva valge raamatu teemaderingist välja.
[8] COM(2019) 168.

Kui rakendada ELi suutlikkust investeerida järgmise põlvkonna tehnoloogiasse ja taristusse, samuti sellistesse digioskustesse nagu andmekirjaoskus, suurendab see Euroopa tehnoloogilist sõltumatust andmepõhist majandust võimaldava keskse tähtsusega tehnoloogia ja taristu alal. Taristu peaks toetama selliste Euroopa andmekogumite loomist, mis panevad aluse usaldusväärsele, st Euroopa väärtustel ja normidel põhinevale tehisintellektile.

Euroopa peaks kasutama oma tugevaid külgi, et kindlustada oma positsiooni ökosüsteemides ja kogu väärtusahela ulatuses, see tähendab nii teatavates riistvara tootmise sektorites kui ka tarkvara ja teenuste vallas. Teatud määral seda juba tehakse. Euroopas valmistatakse üle veerandi kõigist tööstus- ja teenindusrobotitest (nt täppispõllunduse ning julgeoleku-, tervishoiu- ja logistikavaldkonna jaoks) ning liidul on oluline roll ettevõtetele ja organisatsioonidele mõeldud tarkvara (ettevõtjatevahelised rakendused, nagu ettevõtte ressursiplaneerimine ning tarkvara projekteerimine ja teostamine), samuti e-riiki ja nn nutiettevõtteid toetavate rakenduste arendamises ja juurutamises.

Tootmissektoris on Euroopa tehisintellekti juurutamise esirinnas. Enam kui pool liidu peamistest tootjatest rakendab tootmistegevuses vähemalt üht tehisintellekti elementi[9].

Euroopa teadusuuringud on heas seisus muu hulgas tänu ELi rahastamisprogrammile, mis on osutunud kasulikuks jõupingutuste liitmisel, dubleerimise vältimisel ning avaliku ja erasektori investeeringute kaasamisel liikmesriikides. Viimase kolme aasta jooksul on ELi rahastus teadustegevusele ja innovatsioonile tehisintellekti vallas jõudnud 1,5 miljardi euroni, st suurenenud võrreldes eelmise perioodiga 70 %.

Kuid Euroopa investeeringud teadustegevusse ja innovatsiooni kujutavad endast siiski ainult murdosa avaliku ja erasektori investeeringutest maailma teistes piirkondades. Kui 2016. aastal investeeriti Euroopas tehisintellekti umbes 3,2 miljardit eurot, siis Põhja-Ameerikas oli investeeringuid umbes 12,1 miljardit ja Aasias 6,5 miljardit eurot [10]. Et sellega sammu pidada, peab Euroopa oma investeeringute taset oluliselt tõstma. Koos liikmesriikidega välja töötatud kooskõlastatud kava, mis käsitleb tehisintellekti, [11] on osutunud heaks lähtepunktiks koostöö süvendamisel Euroopas ja sünergiate loomisel seoses tehisintellekti väärtusahelasse tehtavate investeeringute maksimeerimisega.

3. KASUTAME ÄRA UUED VÕIMALUSED: JÄRGMISE ANDMELAINEGA EDASI

Ehkki praegu on Euroopa tarbijale suunatud rakenduste ja veebiplatvormide vallas teistest nõrgem ja see tingib ebasoodsa konkurentsiolukorra seoses juurdepääsuga andmetele, on toimumas olulised muutused seoses andmete väärtuse ja sektoriülese taaskasutusega. Maailmas toodetavate andmete hulk kasvab kiiresti: kui 2018. aastal oli neid 33 zettabaiti, siis 2025. aastaks jõutakse eelduste kohaselt 175 zettabaidini [12]. Iga uus andmelaine annab Euroopale uusi võimalusi leida oma koht osava andmekasutusega majanduses ja jõuda selles vallas liidripositsioonile. Lisaks sellele muutuvad andmete säilitamine ja töötlemine järgmise viie aasta jooksul drastiliselt. Praegu toimub 80 % pilvepõhisest andmetöötlusest ja -analüüsist andmekeskustes ja tsentraliseeritud andmetöötlussüsteemides ning 20 % ühendatud nutiseadmetes, nagu autod, kodutehnika ja tööstusrobotid, samuti kasutaja läheduses asuvates andmetöötlussüsteemides (nn servtöötlus). 2025. aastaks peaksid see vahekord märkimisväärselt muutuma[13].

[9] Seda on rohkem kui Jaapanis (30 %) ja USAs (28 %). Allikas: CapGemini (2019).
[10] 10 imperatives for Europe in the age of AI and automation (McKinsey, 2017).
[11] COM(2018) 795.
[12] IDC (2019).
[13] Gartner (2017).

Euroopa on üks maailma esinumbreid väikese energiatarbimisega elektroonika alal, mis on keskse tähtsusega tehisintellekti järgmise põlvkonna protsessorite jaoks. Selle valdkonna turgu valitsevad praegu ELi välised osalejad. Olukord võiks muutuda tänu sellistele algatustele nagu Euroopa protsessorialgatus, mis keskendub vähese energiatarbimisega andmetöötlussüsteemide arendamisele nii servtöötluse kui ka järgmise põlvkonna kõrgjõudlusega andmetöötluse jaoks, ning peamiste digitehnoloogia valdkondade ühisettevõte, mis peaks kava kohaselt alustama 2021. aastal. Lisaks on Euroopa liidripositsioonil selliste neuromorfsete lahenduste [14] alal, mis sobivad ideaalselt tööstusprotsesside (Industry 4.0) ja transpordiviiside automatiseerimiseks. Need saavad energiatõhususust kordades suurendada.

Viimase aja edusammud kvantarvutuse alal suurendavad andmetöötlusjõudlust mitmekordselt [15]. Euroopa saab olla selle tehnoloogia esirinnas tänu kõrgele akadeemilisele tasemele kvantarvutuse alal ning Euroopa tööstuse tugevale positsioonile kvantsimulaatorite ja kvantarvutuse programmeerimiskeskkondade valdkonnas. Euroopa algatused, mis on suunatud kvanttehnoloogia katse- ja eksperimenteerimiskeskkondade kättesaadavamaks tegemisele, aitavad rakendada neid uusi kvantlahendusi mitmes tööstus- ja akadeemilises sektoris.

Samal ajal jätkab Euroopa tehisintellekti aluseks olevate algoritmide valdkonna esirinnas, tuginedes oma tipptasemel teadusele. Vaja on luua ühendused selliste praegu eraldi tegutsevate valdkondade vahel nagu masinõpe ja süvaõpe (neid iseloomustavad piiratud tõlgendatavus, vajadus kasutada mudelite treenimiseks suurt hulka andmeid ja korrelatsioonide põhjal õppimine) ning sümboolsed käsitused (mille puhul reeglid loob inimene). Sümbolloogika ja süvaneurovõrkude ühendamine võib aidata meil parandada tehisintellekti kasutamisel saadavate tulemuste selgitatavust.

4. TIPPTASEME ÖKOSÜSTEEM

Selleks et luua tipptaseme ökosüsteem, mis suudab toetada tehisintellekti väljatöötamist ja kasutuselevõttu ELi majanduses ja haldusasutustes, tuleb hoogustada meetmeid väga mitmel tasandil.

A. KOOSTÖÖ LIIKMESRIIKIDEGA

2018. aasta aprillis vastu võetud tehisintellekti strateegia[16] elluviimiseks esitas komisjon 2018. aasta detsembris kooskõlastatud kava, mis on koostatud ühes liikmesriikidega ning mille eesmärk on edendada tehisintellekti arendamist ja kasutamist Euroopas[17].

Kavas tehakse ettepanek võtta ligi 70 ühismeedet tihedamaks ja tulemuslikumaks koostööks liikmesriikide vahel ja komisjoniga sellistes põhivaldkondades nagu teadustegevus, investeeringud, levik turul, oskused ja anded, andmed ja rahvusvaheline koostöö. Kava on planeeritud kestma aastani 2027 ning seda hakatakse korrapäraselt jälgima ja läbi vaatama.

Eesmärk on veelgi suurendada teadustegevusse, innovatsiooni ja juurutamisse tehtavate investeeringute mõju, hinnata riiklike tehisintellektistrateegiaid ning arendada edasi ja laiendada liikmesriikidega kooskõlastatud kava tehisintellekti kohta.

[14] Neuromorfsete lahenduste all mõistetakse väga ulatuslikke integraallülitussüsteeme, mis imiteerivad närvisüsteemis leiduvate neurobioloogiliste süsteemide ülesehitust.
[15] Kvantarvutid suudavad vähem kui sekunditega töödelda palju suuremaid andmekogumeid kui praegused kõige suurema jõudlusega arvutid ja võimaldavad seega välja töötada uusi tehisintellektirakendusi eri sektorites.
[16] Tehisintellekt Euroopa huvides (COM(2018) 237).
[17] Tehisintellekti käsitlev kooskõlastatud kava (COM (2018) 795).

- *Meede 1: komisjon esitab liikmesriikidele kooskõlastatud kava muudatused, mille juures on arvesse võetud valge raamatu teemalise avaliku konsultatsiooni tulemusi ja mis tuleb vastu võtta 2020. aasta lõpuks.*

ELi tasandi rahastus tehisintellektile peaks ligi meelitama ja koondama investeeringuid neis valdkondades, kus on vaja suuremaid jõupingutusi kui ükski liikmesriik eraldi teha suudab. Järgmise kümnendi jooksul on eesmärk kaasata aastas tehisintellekti enam kui 20 miljardit eurot [18] investeeringuid. Selleks et stimuleerida era- ja avaliku sektori investeeringuid, teeb EL vähem arenenud piirkondade ja maapiirkondade vajaduste jaoks kättesaadavaks digitaalse Euroopa programmi, programmi „Euroopa horisont" ning Euroopa struktuuri- ja investeerimisfondide vahendid.

Samuti võiks kooskõlastatud kava käsitleda tehisintellekti keskse põhimõttena ühiskondlikku ja keskkonnaalast heaolu. Tehisintellektisüsteemidest tõotab olla kasu kõige pakilisemate probleemide – nagu kliimamuutused ja keskkonnaseisundi halvenemine – lahendamisel. Seejuures on oluline, et see toimuks keskkonnasõbralikul viisil. Tehisintellekt ise on võimeline ja peab kriitilise pilguga jälgima ressursikasutust ja elektritarbimist ning seda tuleb treenida tegema keskkonna jaoks positiivseid valikuid. Komisjon kaalub võimalusi soodustada ja propageerida koos liikmesriikidega selliste omadustega tehisintellektilahendusi.

B. ANNAME TEADUS- JA INNOVATSIOONIRINGKONDADE JÕUPINGUTUSTELE ÜHE SUUNA

Euroopa ei saa endale lubada, et säiliks praegune olukord, kus pädevuskeskused on laiali pillutatud ja ükski neist ei saavuta sellist taset, mis oleks vajalik maailma tippudega võistlemiseks. Erinevate tehisintellektiga tegelevate Euroopa teaduskeskuste vahel tuleb ilmtingimata luua rohkem sünergiat ja võrgustikke ning anda nende jõupingutustele üks suund, et tõsta nende taset, hoida kinni ja meelitada ligi parimaid teadlasi ning arendada välja parim tehnoloogia. Euroopal on nende jõupingutuste koordineerimiseks vaja keskset teadus-, innovatsiooni- ja ekspertteadmiste keskust, millel peaks olema tehisintellekti valdkonnas maailmamaine ning mis suudaks ligi meelitada investeeringuid ja selle valla kõige helgemaid päid.

Keskused ja võrgustikud peaksid pühendama oma tähelepanu neile sektoritele, kus Euroopal on võimalused saada maailmameistriks, nagu tööstus, tervishoid, transport, rahandus, toidutarne väärtusahelad, energeetika/keskkond, metsamajandus, Maa seire ja kosmos. Kõigis neis valdkondades käib võidujooks maailma liidripositsioonidele ning Euroopal on märkimisväärsed võimalused, teadmised ja oskusteave[19]. Uute tehisintellektirakenduste arendamise ja juurutamise seisukohast on niisama oluline luua katse- ja eksperimenteerimiskeskused.

- *Meede 2: komisjon aitab luua tipp- ja katsekeskused, mis suudavad kokku tuua investeeringuid Euroopa vahenditest, liikmesriikidelt ja erasektorist; selle juurde võib kuuluda uus õigusakt. Mitmeaastase finantsraamistiku (2021–2027) alla kuuluva digitaalse Euroopa programmi raames (mida täiendatakse vajaduse korral programmi „Euroopa horisont" teadusuuringute ja innovatsiooni meetmetega) on komisjon välja pakkunud muljetavaldava sihtotstarbelise summa, et toetada üleilmse mõõdupuu staatusega katsekeskusi Euroopas.*

C. OSKUSED

[18] COM(2018) 237.
[19] Samuti pakuvad tehisintellekti alase uurimis- ja arendustegevuse jaoks võimalusi tulevane Euroopa Kaitsefond ja alaline struktureeritud koostöö (PESCO). Need projektid tuleks kooskõlastada tehisintellektile pühendatud laiemate tsiviilotstarbeliste projektidega ELis.

Euroopa tehisintellektikäsitust peab toetama tugev rõhuasetus oskustele, et korvata pädevate töötajate nappust[20]. Õige pea esitab komisjon tõhustatud tegevuskava oskuste kohta, mille eesmärk on tagada, et kõigil eurooplastel on võimalik saada kasu ELi majanduse keskkonnasäästlikust ja digitaalsest ümberkorraldamisest. Samuti võiks algatuste raames toetada valdkondade reguleerivaid asutusi, et suurendada asjaomaste normide tõhusa ja tulemusliku rakendamise eesmärgil nende tehisintellekti alaseid oskusi. Digiõppe ajakohastatud tegevuskava aitab paremini kasutada andme- ja tehisintellektipõhist tehnoloogiat (nagu õpe ja prognoosiv analüütika), et parandada haridus- ja koolitussüsteeme ning muuta need digiajastule vastavaks. Samuti suurendatakse kava abil tehisintellekti alast teadlikkust kõigil haridustasemetel, et valmistada kodanikke ette tegema teadlikke valikuid, mida tehisintellekt üha enam mõjutab.

Tehisintellekti käsitleva kooskõlastatud kava läbivaadatud versioonis, mis töötatakse välja koos liikmesriikidega, on üks olulisemaid teemasid tehisintellekti valdkonnas töötamiseks vajalike oskuste arendamine ja tööjõu ettevalmistamine tehisintellekti juhitavateks muutusteks. Selle raames võiks eetiliste suuniste kontrollnimekirja põhjal koostada orienteeruva õppekava tehisintellekti arendajatele, mis antaks õppematerjalina koolitusasutuste käsutusse. Erilisi jõupingutusi tuleks teha selleks, et suurendada selles valdkonnas haridust ja tööd saavate naiste arvu.

Peale selle tõmbaks tehisintellekti alase teadustöö ja innovatsiooni tippkeskus Euroopas oma pakutavate võimalustega ligi talente kogu maailmast. Samuti arendaks ja levitaks see kõikjal Euroopas kanda kinnitavaid ja arenevaid tipptasemel oskusi.

- *Meede 3: luua digitaalse Euroopa programmi kõrgtasemel oskuste samba abil juhtivate ülikoolide ja kõrgharidusasutuste võrgustikud ja toetada neid, et meelitada ligi parimaid õppejõude ja teadlasi ning pakkuda maailma tipptasemel magistriõppeprogramme tehisintellekti alal.*

Lisaks oskuste täiendamisele mõjutab töötajaid ja tööandjaid otseselt tehisintellektisüsteemide projekteerimine ja kasutamine töökohal. Sotsiaalpartnerite osalus on väga oluline selleks, et tagada inimesekeskne lähenemine tehisintellektile töökeskkonnas.

D. TÄHELEPANU KESKMES ON VKED

Samuti on oluline tagada, et VKEdel oleks juurdepääs tehisintellektile ja võimalus seda kasutada. Selleks tuleks veelgi tugevdada digitaalse innovatsiooni keskusi[21] ja tehisintellektialase nõudeteenuse platvormi,[22] mis peaksid soodustama VKEde vahelist koostööd. Selle saavutamisel mängib suurt rolli digitaalse Euroopa programm. Ehkki kõik digitaalse innovatsiooni keskused peaksid pakkuma VKEdele tehisintellekti mõistmise ja kasutuselevõtu alast toetust, peaks vähemalt üks innovatsioonikeskus liikmesriigi kohta olema spetsialiseerunud just tehisintellektile.

VKEdel ja idufirmadel peab oma protsesside kohandamiseks ja tehisintellektil põhinevaks innovatsiooniks olema juurdepääs rahastamisele. Komisjonil on plaanis suurendada rahastamisvõimalusi tehisintellekti valdkonnas InvestEU programmi [23] raames veelgi, tuginedes loodavale 100 miljoni euro suurusele katsefondile, mis on mõeldud tehisintellekti ja plokiahelasse

[20] https://ec.europa.eu/jrc/en/publication/academic-offer-and-demand-advanced-profiles-eu.
[21] ec.europe.eu/digital-single-market/en/news/digital-innovation-hubs-helping-companies-across-economy-make-most-digital-opportunities.
[22] www.Ai4eu.eu.
[23] Europe.eu/investeu.

investeerimiseks. InvestEU tagatise saamiseks sobilike valdkondade seas on tehisintellekt eraldi ära nimetatud.

- *Meede 4: komisjon teeb liikmesriikidega koostööd, et tagada vähemalt ühe tehisintellektile spetsialiseerunud digitaalse innovatsiooni keskuse olemasolu igas liikmesriigis. Digitaalse innovatsiooni keskuseid saab toetada digitaalse Euroopa programmist*.
- *2020. aasta esimeses kvartalis algatavad komisjon ja Euroopa Investeerimisfond 100 miljoni euro suuruse katseprojekti, et rahastada omakapitali kaudu tehisintellekti alaseid uuenduslikke arendusi. Eeldusel, et saavutatakse lõplik kokkulepe mitmeaastase finantsraamistiku kohta, kavatseb komisjon summat alates 2021. aastast InvestEU vahenditest märkimisväärselt suurendada.*

E. PARTNERLUS ERASEKTORIGA

Samuti tuleb kindlustada, et erasektor on täielikult kaasatud teadusuuringute ja innovatsiooni tegevuskava koostamisse ning teeb vajalikul määral kaasinvesteeringuuid. Selleks on vaja luua laiapõhjaline avaliku ja erasektori partnerlus ning kindlustada ettevõtete tippjuhtide toetus.

- *Meede 5: komisjon loob programmi „Euroopa horisont“ raames uue avaliku ja erasektori partnerluse tehisintellekti, andmete ja robootika vallas, et koondada jõupingutusi, tagada tehisintellekti alaste teadusuuringute ja innovatsiooni kooskõlastamine, teha koostööd muude programmi „Euroopa horisont“ alla kuuluvate avaliku ja erasektori partnerlusprojektidega ning töötada koos katsekeskuste ja digitaalse innovatsiooni keskustega, mida eespool mainiti.*

F. PROPAGEERIME TEHISINTELLEKTI KASUTUSELEVÕTTU AVALIKUS SEKTORIS

On väga oluline, et haldusasutused, haiglad, kommunaal- ja transporditeenused, finantsjärelevalveasutused ja muud avalikku huvi pakkuvad valdkonnad hakkaksid kiiresti oma tegevusse juurutama tehisintellekti põhiseid tooteid ja teenuseid. Erilise tähelepanu all on tervishoid ja transport, kus tehnoloogia on ulatuslikuks juurutamiseks valmis.

- *Meede 6: komisjon algatab avatud ja läbipaistvad valdkondliku dialoogid – esmajärjekorras tervishoiusektori, maapiirkondade haldusüksuste ja avalike teenuste osutajatega –, et esitada tegevuskava arendustegevuse, eksperimenteerimise ja kasutuselevõtu hõlbustamiseks. Valdkondlike dialoogide varal valmistatakse ette spetsiaalne programm „Võtame tehisintellekti kasutusele“, mis toetab tehisintellektisüsteemidele keskenduvaid avalikke hankeid ja aitab muuta ka avalike hangete protsesse.*

G. TAGAME JUURDEPÄÄSU ANDMETELE JA ANDMETÖÖTLUSTARISTUTELE

Käesolevas valges raamatus loetletud tegevusvaldkonnad täiendavad kava, mis esitati sellega ühel ajal Euroopa andmestrateegia raames. Määrava tähtsusega on parandada juurdepääsu andmetele ja nende haldamist. Andmeteta on tehisintellekti ja muude digirakenduste arendamine võimatu. Tulevikus genereeritav tohutu hulk uusi andmeid annab Euroopale võimaluse asuda andmepõhisusele ja tehisintellektile ülemineku esirinda. Vastutustundlike andmehaldustavade propageerimine ja andmete kooskõla FAIR-põhimõtetega aitab luua usaldust ja tagab andmete taaskasutatavuse[24]. Niisama oluline on investeerida peamisesse andmetöötlustehnoloogiasse ja -taristusse.

Komisjon on teinud ettepaneku toetada kõrgjõudlusega andmetöötlust ja kvantarvutust (sealhulgas servtöötlust, tehisintellekti ning andme- ja pilvetaristut) digitaalse Euroopa programmist enam kui 4 miljardi euroga. Euroopa andmestrateegia raames arendatakse neid põhivaldkondi edasi.

H. RAHVUSVAHELISED ASPEKTID

Euroopal on head eeldused olla üleilmne liider jagatud väärtuste põhiste liitude ehitamisel ja tehisintellekti eetilise kasutamise propageerimisel. ELi töö tehisintellekti vallas on juba mõjutanud rahvusvahelisi arutelusid. Kõrgetasemeline eksperdirühm kaasas oma eetiliste suuniste väljatöötamisse hulga ELi väliseid organisatsioone ja mitu valitsuse tasandi vaatlejat. Samal ajal oli EL tihedalt seotud tehisintellekti käsitlevate OECD eetikapõhimõtete väljatöötamisega[25]. G20 kinnitas need põhimõtted oma 2019. aasta juunikuise ministrite avaldusega kaubanduse ja digitaalmajanduse kohta.

Samal ajal tunnustab EL olulist tööd, mis toimub muudel mitmepoolsetel foorumitel, sealhulgas Euroopa Nõukogus, ÜRO Hariduse, Teaduse ja Kultuuri Organisatsioonis (UNESCO), Majanduskoostöö ja Arengu Organisatsioonis (OECD), Maailma Kaubandusorganisatsioonis ja Rahvusvahelises Telekommunikatsiooni Liidus. ÜROs on EL tegev digitaalvaldkonna koostöö kõrgetasemelise eksperdirühma aruande järelmeetmete vallas, muu hulgas seoses soovitusega tehisintellekti kohta.

EL jätkab tehisintellekti alast koostööd samal meelel olevate riikide, kuid ka rahvusvaheliste osalistega, tuginedes lähenemisviisile, mis põhineb sellistel ELi normidel ja väärtustel nagu toetus

[24] Leitavad, juurdepääsetavad, koostalitlusvõimelised ja taaskasutatavad andmed (*findable, accessible, interoperable and reusable* – FAIR), nagu on sätestatud komisjoni ekspertrühma lõplikus aruandes ja tegevuskavas FAIR andmete kohta (2018), https://ec.europa.eu/info/sites/info/files/turning_fair_into_reality_1.pdf.

[25] https://www.oecd.org/going-digital/ai/principles/.

ülespoole suunatud õigusnormide lähendamisele, juurdepääs peamistele ressurssidele – nende hulgas on andmed – ja võrdsete võimaluste loomine. Komisjon jälgib tähelepanelikult andmevooge piiravate kolmandate riikide poliitikat ja võtab põhjendamatud piirangud käsile kahepoolsete kaubandusläbirääkimiste raames ning meetmetega Maailma Kaubandusorganisatsiooni kontekstis. Komisjon on veendunud, et tehisintellekti teemaline rahvusvaheline koostöö peab põhinema käsitusel, mis propageerib austust selliste põhiõiguste vastu nagu inimväärikus, pluralism, kaasatus, diskrimineerimiskeeld ning eraelu puutumatuse ja isikuandmete kaitse,[26] ja püüdleb selle poole, et levitada oma väärtusi kõikjal maailmas[27]. Samuti on selge, et tehisintellekti vastutustundlik arendamine ja kasutamine võivad olla liikumapanevaks jõuks kestliku arengu eesmärkide saavutamise ja 2030. aasta tegevuskava alaste edusammude juures.

5. USALDUSVÄÄRNE ÖKOSÜSTEEM: TEHISINTELLEKTI ÕIGUSRAAMISTIK

Nagu iga uue tehnoloogia puhul, kaasnevad ka tehisintellekti kasutamisega nii uued võimalused kui ka uued riskid. Kodanikud kardavad, et seistes silmitsi algoritmipõhise otsustamisprotsessiga kaasneva informatsiooni asümmeetriaga, on nad võimetud oma õigusi ja turvalisust kaitsma, ettevõtetele teeb aga muret õiguskindlusetus. Ehkki tehisintellektist võib olla abi kodanike turvalisuse kaitsel ja nende põhiõiguste tagamisel, teevad kodanikele teisalt muret tehisintellekti võimalikud soovimatud tagajärjed või isegi selle potentsiaalne kuritahtlik kasutamine. Nende muret tuleb tõsiselt võtta. Lisaks investeeringute ja oskuste nappusele on peamine tehisintellekti ulatuslikumat kasutuselevõttu kammitsev tegur usalduse puudus.

Seetõttu esitas komisjon 25. aprillil 2018 tehisintellekti strateegia,[28] milles käsitletakse lisaks investeeringute suurendamisele teadusuuringutesse, innovatsiooni ja tehisintellektisuutlikkusse kõikjal ELis ka tehisintellekti kasutuselevõtmise sotsiaalmajanduslikke aspekte. Ta leppis liikmesriikidega kokku strateegiate ühitamisele suunatud kooskõlastatud kava[29]. Samuti kutsus komisjon kokku kõrgetasemelise eksperdirühma, mis avaldas 2019. aasta aprillis suunised usaldusväärse tehisintellekti kohta[30].

Komisjon avaldas teatise,[31] millega ta kiitis heaks kõrgetasemelise eksperdirühma suunistes esitatud seitse peamist nõuet:

- inimese toimevõime (*human agency*) ja järelevalve;
- tehniline töökindlus ja ohutus;
- privaatsus ja andmehaldus;
- läbipaistvus;
- mitmekesisus, mittediskrimineerimine ja õiglus;
- ühiskondlik ja keskkonnaalane heaolu;
- vastutuse võtmine.

Lisaks sellele sisaldavad suunised kontrollnimekirja, mida ettevõtted saavad kasutada praktilistel eesmärkidel. 2019. aasta teises pooles on üle 350 organisatsiooni seda kontrollnimekirja kasutanud ja

[26] Komisjon rahastab partnerluse rahastamisvahendist 2,5 miljoni eurose eelarvega projekti, mis hõlbustab koostööd ühel meelel olevate partneritega, et edendada ELi eetilisi suuniseid tehisintellekti kohta ning võtta vastu ühised põhimõtted ja tegevusjäreldused.
[27] President von der Leyen „Liit, mis seab kõrgemad sihid: Minu tegevuskava Euroopa jaoks“ (lk 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.

selle kohta tagasisidet andnud. Kõrgetasemeline eksperdirühm vaatab praegu oma suuniseid uuesti läbi selle tagasiside valguses ja viib selle töö lõpule 2020. aasta juuniks. Tagasisideprotsessi oluline järeldus on see, et ehkki juba praegu kajastuvad olemasolevates õiguslikes või reguleerivates süsteemides paljud nõuded, puuduvad kehtivates õigusaktides konkreetsed sätted läbipaistvuse, jälgitavuse ja inimjärelevalve kohta seoses paljude majandussektoritega.

Lisaks neile kõrgetasemelise eksperdirühma mittesiduvatele suunistele ja kooskõlas presidendi poliitiliste suunistega suurendaks Euroopa selge õigusraamistik tarbijate ja ettevõtete usaldust tehisintellekti vastu ning kiirendaks seega tehnoloogia kasutuselevõttu. Selline õigusraamistik peaks olema kooskõlas muude meetmetega Euroopa innovatsioonisuutlikkuse ja konkurentsivõime edendamiseks käesolevas valdkonnas. Lisaks peab see tagama ühiskonna, keskkonna ja majanduse seisukohast optimaalse tulemuse ning kooskõla ELi õigusnormide, põhimõtete ja väärtustega. See on eriti oluline valdkondades, kus mõju kodanike õigustele võib olla kõige otsesem, näiteks juhul kui tehisintellektirakendusi kasutatakse õiguskaitses ja kohtumõistmises.

Tehisintellekti arendajate ja juurutajate suhtes kehtivad juba praegu Euroopa õigusaktid, mis puudutavad põhiõigusi (näiteks andmekaitse, privaatsus ja diskrimineerimiskeeld), tarbijakaitse-eeskirjad ning normid tooteohutuse ja tootjavastutuste kohta. Tarbijad ootavad toodetelt ja süsteemidelt ühetaolist ohutust ja nende õiguste austamist sõltumata sellest, kas nende juures kasutatakse tehisintellekti või mitte. Kuid teatavad tehisintellekti eriomadused, nagu läbipaistmatus, võivad nende õigusaktide kohaldamist ja täitmise tagamist raskendada. Sel põhjusel tuleb uurida, kas kehtivad õigusaktid suudavad tehisintellekti riske käsitleda ja kas nende täitmist on võimalik tulemuslikult tagada, kas õigusakte on vaja kohandada või kas on vaja uusi õigusakte.

Võttes arvesse seda, kui kiiresti tehisintellekt areneb, peab õigusraamistik võimaldama arvesse võtta uusi muutusi. Muudatused peaksid piirduma selgelt kindlakstehtud probleemidega, mille jaoks on olemas teostatavad lahendused.

Liikmesriigid juhivad tähelepanu sellele, et praegu puudub Euroopa ühine raamistik. Saksa andme-eetika komisjon on kutsunud üles looma viieastmelise riskipõhise regulatiivse süsteemi: selle esimesel astmel oleksid kõige ohutumad tehisintellektisüsteemid, mida ei reguleeritaks, ja viimasel kõige ohtlikumad, mis keelataks täielikult. Taani käivitas äsja andme-eetika märgise prototüübi. Malta on kehtestanud tehisintellekti vabatahtliku sertifitseerimissüsteemi. Kui EL ei suuda välja pakkuda ELi-ülest käsitust, eksisteerib reaalne oht siseturu killustumiseks, mis takistaks usalduse, õiguskindluse ja turul levimise eesmärkide saavutamist.

Usaldusväärse tehisintellekti kindel Euroopa õigusraamistik kaitseb Euroopa kodanikke ja aitab luua tõrgeteta toimiva siseturu tehisintellekti edasiarendamise ja kasutuselevõtu jaoks, tugevdades ka Euroopa tehisintellekti valdkonna tööstusbaasi.

A. PROBLEEMI MÄÄRATLUS

Tehisintellekt võib teha palju head, sealhulgas muuta tooted ja protsessid turvalisemaks, kuid võib teha ka kahju. Kahju võib olla nii materiaalne (kahju inimeste turvalisusele ja tervisele, sealhulgas surmajuhtumid, varaline kahju) kui ka mittemateriaalne (privaatsuse kaotus, väljendusvabaduse õiguse või inimväärikuse piiramine, diskrimineerimine näiteks seoses juurdepääsuga tööhõivele) ja võib seonduda väga erinevate riskidega. Õigusraamistiku fookuses peaks olema see, kuidas viia erinevate riskide võimalus miinimumini, eriti mis puudutab kõige suuremaid riske.

Peamised tehisintellekti kasutamisega seotud riskid puudutavad selliste normide kohaldamist, mis on ette nähtud põhiõiguste kaitseks (sealhulgas isikuandmete ja privaatsuse kaitse ning diskrimineerimiskeeld), samuti ohutuse[32] ja tootjavastutusega seotud küsimusi.

Riskid, mis on seotud põhiõigustega, ennekõike isikuandmete ja privaatsuse kaitse ning diskrimineerimiskeeluga

Tehisintellekti kasutamine võib kahjustada väärtusi, millele EL on rajatud, ja rikkuda põhiõigusi,[33] sealhulgas õigust väljendusvabadusele, kogunemisvabadusele ja inimväärikusele, keeldu diskrimineerida soo, rassilise või etnilise päritolu, usutunnistuse või veendumuste, puuete, vanuse või seksuaalse sättumuse alusel (sõltuvalt valdkonnast), isikuandmete ja eraelu kaitset,[34] õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumõistmisele, samuti tarbijakaitsenorme. Need riskid võivad olla tingitud vigadest selles, kuidas tehisintellektisüsteemid on projekteeritud (sealhulgas seoses inimjärelevalvega), või andmete kasutamisest ilma, et oleks korrigeeritud võimalikku kallutatust (näiteks on süsteemi treenitud ainult või peamiselt meestelt pärinevate andmetega, mistõttu naiste puhul ei ole saadavad tulemused optimaalsed).

Tehisintellekt suudab sooritada paljusid ülesandeid, mida minevikus suutis ainult inimene. Selle tulemusena kohaldatakse kodanike ja juriidiliste isikute suhtes tehisintellekti või selle abi kasutades üha enam meetmeid ja tehakse otsuseid, mida võib aeg-ajalt olla raske mõista ja vajaduse korral tulemuslikult vaidlustada. Lisaks sellele suurendab tehisintellekt võimalusi inimeste igapäevaharjumusi registreerida ja analüüsida. Näiteks on oht, et tehisintellekti võidakse kasutada ELi andmekaitse- ja muid norme rikkudes riiklike ametiasutuste või muude üksuste poolseks massijälgimiseks või tööandjate poolseks töötajate käitumise jälgimiseks. Suurte andmehulkade analüüsi ja nendevaheliste seoste leidmise varal saab tehisintellekti kasutada ka isikuandmete leidmiseks ja nende taasidentifitseerimiseks, mistõttu tekivad uued isikuandmete kaitsega seotud riskid isegi selliste andmekogumite puhul, mis iseenesest isikuandmeid ei sisalda. Samuti kasutavad tehisintellekti veebipõhised vahendajad, kes järjestavad selle abil oma kasutajatele suunatud teavet ja modereerivad sisu. Töödeldud andmed, rakenduste ülesehitus ja see, mil määral inimene sekkub, võivad mõjutada õigust väljendusvabadusele, isikuandmete kaitsele ja privaatsusele ning poliitilisi vabadusi.

[32] Siia kuuluvad küsimused, mis puudutavad küberturvalisust, tehisintellekti kasutamist elutähtsates taristutes või tehisintellekti kuritarvitamist.

[33] Euroopa Nõukogu uuringust selgub, et tehisintellekti kasutamine võib mõjutada suurt hulka põhiõigusi (https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5).

[34] Neid riske käsitletakse isikuandmete kaitse üldmääruses ja e-privaatsuse direktiivis (uus e-privaatsuse määrus on läbirääkimisel), kuid on võimalik, et tuleb uurida, kas tehisintellektisüsteemidega kaasnevad lisariskid. Komisjon jälgib ja hindab pidevalt isikuandmete kaitse üldmääruse kohaldamist.

Kui kasutada teatavaid tehisintellekti algoritme korduvkuritegevuse prognoosimiseks, võivad tulemused olla sooliselt ja rassiliselt kallutatud ning kuritegude kordumise tõenäosuse prognoos naiste ja meeste või riigi kodanike ja välismaalaste puhul erinev. *Allikas: Tolan S., Miron M., Gomez E. ja Castillo C. „Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia", Parima uurimuse auhind, International Conference on AI and Law, 2019.*

Teatavate tehisintellekti kasutavate näotuvastusprogrammide tulemused on sooliselt ja rassiliselt kallutatud: heledanahaliste meeste soo määramisel on nende veamäär madal, kuid tumedanahaliste naiste soo määramisel kõrge. Allikas: *Joy Buolamwini, Timnit Gebru „Proceedings of the 1st Conference on Fairness, Accountability and Transparency", PMLR 81:77-91, 2018*.

Kallutatuse ja diskrimineerimise risk on lahutamatult seotud mistahes ühiskondliku ja majandusliku tegevusega. Vigade ja kallutatuse eest ei ole kaitset ka inimese tehtud otsuste puhul. Kuid kui seesama kallutatus esineb tehisintellektis, võivad sellel olla palju ulatuslikumad tagajärjed, mis puudutavad ja diskrimineerivad paljusid inimesi ilma, et käivituksid inimeste käitumist reguleerivad sotsiaalse kontrolli mehhanismid[35]. See võib juhtuda ka siis, kui tehisintellektisüsteem nn õpib tegevuse käigus. Juhul kui tulemusi ei oleks saanud projekteerimisetapis vältida ega ennetada, ei tulene riskid mitte veast süsteemi algses projektis, vaid süsteemi poolt suures andmekogumis identifitseeritud korrelatsioonide või kujundite praktilisest mõjust.

Tehisintellekti erinevate väljundite eriomadused, sealhulgas läbipaistmatus (nn musta kasti efekt), keerukus, ettearvamatus ja osaliselt autonoomne tegutsemine, võivad luua olukorra, kus on ülimalt raske kontrollida kooskõla põhiõiguste kaitseks mõeldud olemasolevate ELi õigusaktidega, ja pärssida nende täitmise tulemuslikku tagamist. Ei täitevasutustel ega puudutatud isikutel pruugi olla vahendeid, et kontrollida, kuidas jõuti konkreetse otsuseni, mille tegemisse oli kaasatud tehisintellekt, ja niisiis seda, kas asjaomastest normidest peeti kinni või mitte. Füüsilistel ja juriidilistel isikutel võib tekkida raskusi tulemusliku juurdepääsuga õigusemõistmisele olukordades, kus sellistel otsustel võib olla neile negatiivne mõju.

Turvalisust ja tootjavastutuse tulemuslikku toimimist ohustavad riskid

Kui tehisintellektitehnoloogia on toodetesse ja teenustesse sisse ehitatud, võib see tingida uusi riske kasutajate turvalisusele. Näiteks vea tõttu eseme tuvastamistehnoloogias võib isejuhtiv auto tuvastada valesti teel oleva objekti ning põhjustada õnnetuse, millega kaasnevad kehavigastused ja materiaalne kahju. Mis puudutab põhiõigustega seotud riske, võivad need tuleneda vigadest tehisintellektitehnoloogia ülesehituses või olla seotud kas andmete kättesaadavuse ja kvaliteedi problemaatilisuse või siis muude masinõppest tulenevate probleemidega. Ehkki mõned neist riskidest

[35] Komisjoni meeste ja naiste võrdsete võimaluste nõuandekomitee valmistab praegu ette arvamust tehisintellekti kohta, milles analüüsitakse muu hulgas tehisintellekti mõju soolisele võrdõiguslikkusele ja mille komitee peaks vastu võtma 2020. aasta alguses. Samuti käsitletakse tehisintellekti ja soolise võrdõiguslikkuse vahelist seost ELi soolise võrdõiguslikkuse strateegias aastateks 2020–2024; Euroopa Liidu võrdõiguslikkust edendavate asutuste võrgustik (EQUINET) avaldab aruande, mille autorid on Robin Allen ja Dee Masters ning teema „Tehisintellekti reguleerimine: võrdõiguslikkust edendavate asutuste uus roll. Suurenevast digiteerimisest ja tehisintellekti kasutamisest tulenevate võrdsuse ja diskrimineerimiskeeluga seotud probleemide käsitlemine" („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"), mis peaks valmima 2020. aasta alguses.

ei esine sugugi ainult tehisintellekti kasutavate toodete ja teenuste puhul, võib tehisintellekti kasutamine suurendada riskide tõenäosust või nende raskusastet.

Nende riskide vastaste selgete ohutusnõuete puudumine võib lisaks asjaomaste isikute ohtu seadmisele tingida õiguskindlusetuse selliste ettevõtete jaoks, kes turustavad ELis oma tooteid, milles kasutatakse tehisintellekti. Turujärelevalve- ja täitevasutused võivad avastada end olukorrast, kus pole selge, kas nad tohivad sekkuda, kuna neil ei pruugi olla tegutsemisvolitusi ja/või asjakohast tehnilist pädevust süsteemide inspekteerimiseks[36]. Õiguskindlusetus võib seega vähendada üldist turvalisuse taset ja kahjustada Euroopa ettevõtete konkurentsivõimet.

Ohutusriskide realiseerumise korral on selgete nõuete puudumise ja tehisintellekti eespool nimetatud omaduste tõttu raske jõuda tehisintellektisüsteemide osalusel tehtud problemaatiliste otsuste allikani. See omakorda raskendab kahju kannatanud isikutel kompensatsiooni saamist kehtivate ELi ja riiklike vastutusalaste õigusaktide alusel[37].

Tootevastutuse direktiivi kohaselt vastutab puudusega toote põhjustatud kahju eest tootja. Kuid selliste tehisintellektipõhiste süsteemide puhul nagu isejuhtivad autod võib olla keeruline tõendada, et tootel on puudus, et tekkinud on kahju ja et nende kahe vahel on põhjuslik seos. Lisaks sellele valitseb teatav ebakindlus seoses sellega, kuidas ja millises ulatuses kohaldada tootjavastutuse direktiivi teatavate puuduste suhtes, näiteks juhul kui need tulenevad nõrkustest toote küberturvalisuses.

Seega esinevad eespool põhiõiguste kontekstis mainitud raskused jõuda tehisintellektisüsteemide tehtud potentsiaalselt problemaatiliste otsuste allikani ka turvalisuse ja vastutusega seotud küsimuste puhul. Kahju kannatanud isikud ei pruugi näiteks saada reaalset juurdepääsu tõenditele, mis on vajalikud kohtuasja ettevalmistamiseks, ja nende käsutuses olevad õiguskaitsevahendid ei puugi olla sama tulemuslikud kui tavatehnoloogia põhjustatud kahju puhul. Tehisintellekti levides need riskid suurenevad.

B. VÕIMALIKUD KOHANDUSED ELI KEHTIVAS ÕIGUSRAAMISTIKUS, MIS PUUDUTAB TEHISINTELLEKTI

Olemas on ulatuslik kogum ELi õigusakte tooteohutuse ja tootjavastutuse kohta,[38] sealhulgas sektoripõhised normid – mida täiendavad riiklikud õigusaktid –, mis on paljude kujunemisjärgus tehisintellektirakenduste puhul asjakohane ja potentsiaalselt nende suhtes kohaldatav.

Põhiõiguste ja tarbijate õiguste kaitse vallas kuuluvad ELi õigusraamistikku sellised õigusaktid nagu rassilise võrdõiguslikkuse direktiiv,[39] direktiiv võrdse kohtlemise kohta töö saamisel ja kutsealale pääsemisel,[40] direktiivid meeste ja naiste võrdse kohtlemise kohta töö saamisel ning kaupade ja

[36] Näiteks võib tuua lastele mõeldud nutikella. Selline toode ei kahjusta otseselt last, kes seda kannab, kuid kuna see ei vasta minimaalsetele turvanõuetele, siis saab seda kergesti kasutada vahendina lapsega suhtlemiseks. Turujärelevalveasutustel võib olla raske tegutseda juhtudel, kui risk ei ole seotud toote kui sellisega.

[37] Käesoleva valge raamatu juurde kuuluvas komisjoni aruandes on analüüsitud tehisintellekti, asjade interneti ja muu digitehnoloogia tähendust ohutus- ja vastutusalaste õigusaktide seisukohast.

[38] ELi tooteohutuse õigusraamistik koosneb nn turvavõrgust, milleks on üldise tooteohutuse direktiiv (direktiiv 2001/95/EÜ), ja hulgast sektoripõhistest normidest, mis hõlmavad erinevaid tootekategooriaid masinatest, lennukitest ja autodest mänguasjade ja meditsiiniseadmeteni ning mille eesmärk on tagada tervisekaitse ja ohutuse kõrge tase. Tootjavastutust käsitlevaid õigusakte täiendavad erinevad tsiviilvastutussüsteemid toodete või teenuste tekitatud kahju puhuks.

[39] Direktiiv 2000/43/EÜ.

[40] Direktiiv 2000/78/EÜ.

teenustele juurdepääsul,[41] mitmed tarbijakaitse-eeskirjad,[42] samuti normid isikuandmete kaitse ja privaatsuse kohta, eriti isikuandmete kaitse üldmäärus ja muud sektoripõhised õigusaktid andmekaitse kohta, nagu direktiiv isikuandmete kaitse kohta õiguskaitse valdkonnas[43]. Lisaks hakkavad alates 2025. aastast kehtima Euroopa ligipääsetavuse aktis sätestatud normid toodete ja teenuste kättesaadavusnõuete kohta[44]. Samuti tuleb põhiõigusi austada muid ELi õigusakte rakendades, sealhulgas finantsteenuste, rände või veebipõhiste vahendajate vastutuse valdkonnas.

Ehkki põhimõtteliselt jäävad ELi õigusaktid tehisintellekti kaasatusest sõltumata täielikult kohaldatavaks, tuleb kindlasti hinnata, kas on võimalik tagada nende asjakohane täitmine tehisintellektist tingitud riskide käsitlemiseks või kas on vaja kohandada konkreetseid õiguslikke vahendeid.

Näiteks jäävad majandustegevuses osalejad täielikult vastutavaks tehisintellekti vastavuse eest kehtivatele tarbijakaitsenormidele, keelatud on tarbijakäitumise ärakasutamine algoritmide abil, rikkudes kehtivaid õigusnorme, ja rikkumiste puhul rakendatakse asjakohaseid karistusi.

Komisjon on seisukohal, et õigusraamistikku saaks parandada, et tulla toime järgmiste riskide ja olukordadega.

- *ELi ja liikmesriikide kehtivate õigusaktide tulemuslik rakendamine ja täitmise tagamine*: tehisintellekti põhiomadused tingivad probleeme ELi ja liikmesriikide õigusaktide nõuetekohase kohaldamise ja täitmise tagamise seisukohast. Läbipaistvuse puudumine (tehisintellekti läbipaistmatus) raskendab võimalike õigusrikkumiste tuvastamist ja tõendamist, muu hulgas selliste seadussätete rikkumiste puhul, millega kaitstakse põhiõigusi, vastutuse määramist ja kahjunõuete esitamise tingimuste täitmist. Seega on võimalik, et õigusnormide tulemuslikuks kohaldamiseks ja täitmise tagamiseks on vaja teatavate valdkondade kehtivaid õigusakte kohandada või täpsustada, näiteks seoses vastutusega, nagu on täpsemalt kirjeldatud käesoleva valge raamatu juurde kuuluvas aruandes.

- *ELi kehtivate õigusaktide kohaldamisala piiratus*: ELi tooteohutusalaste õigusaktide tähelepanu keskmes on eeskätt toodete turule laskmine. Kuigi tarkvara, mis on osa lõpptootest, peab ELi tooteohutusalaste õigusaktide kohaselt vastama asjaomastele tooteohutusnõuetele, puudub vastus küsimusele, kas tooteohutust käsitlevad ELi õigusaktid kehtivad autonoomse tarkvara suhtes, mis ei kuulu teatavatesse selgelt sätestatud normidega sektoreisse[45]. Praegu kehtivaid üldiseid ohutusalaseid ELi õigusakte kohaldatakse toodete ja mitte teenuste suhtes ning seega ei kehti need põhimõtteliselt ka selliste tehisintellektitehnoloogial põhinevate teenuste puhul nagu tervise-, finants- ja transporditeenused.

- *Tehisintellektisüsteemide funktsioonide muutumine*: tarkvara, sh tehisintellekti integreerimine toodetesse võib muuta nende toodete ja süsteemide funktsioone nende elutsükli jooksul. Eriti

[41] Direktiiv 2004/113/EÜ; Direktiiv 2006/54/EÜ.
[42] Näiteks ebaausate kaubandustavade direktiiv (direktiiv 2005/29/EÜ) ja tarbija õiguste direktiiv (direktiiv 2011/83/EÜ).
[43] Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta direktiiv (EL) 2016/680, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist.
[44] Direktiiv (EL) 2019/882 toodete ja teenuste ligipääsetavusnõuete kohta.
[45] Näiteks kui tootja on tarkvara puhul näinud ette selle kasutamise meditsiinilisel eesmärgil, loetakse seda meditsiiniseadmete määruse (määrus (EL) 2017/745) kohaselt meditsiiniseadmeks.

on see nii süsteemide puhul, mis vajavad sagedasi tarkvarauuendeid või mille puhul kasutatakse masinõpet. Need omadused võivad tingida uusi riske, mis ei eksisteerinud süsteemi turule laskmisel. Kuna olemasolevates õigusaktides keskendutakse eelkõige turule laskmise ajal eksisteerivatele riskidele, ei käsitleta neis piisavalt selliseid uusi riske.

- *Ebakindlus seoses vastutuse jaotusega erinevate tarneahelasse kuuluvate majandustegevuses osalejate vahel*: ELi tooteohutusalaste õigusaktide kohaselt vastutab turule lastud toote (sealhulgas kõigi komponentide, näiteks tehisintellektisüsteemide) eest üldiselt selle valmistaja. Kuid normid võivad muutuda ebaselgeks näiteks juhul, kui tehisintellekti lisab tootele pärast selle turule laskmist keegi muu kui toote valmistaja. Lisaks sellele on tootja vastutust käsitlevate ELi õigusaktidega ette nähtud tootjavastutus ja muude tarneahela osaliste vastutus on jäetud liikmesriikide vastutusalaste normide reguleerimisalasse.

- *Ohutuse mõiste muutmine*: tehisintellekti kasutamine toodete ja teenuste puhul võib tingida riske, mida ei ole ELi õigusaktides praegu sõnaselgelt käsitletud. Riskid võivad olla seotud küberohtudega, riskidega üksikisiku turvalisusele (mis on näiteks seotud tehisintellekti uute kasutusviisidega näiteks kodumasinates), ühenduse katkemisest tulenevate riskidega jne. Nimetatud riskid võivad eksisteerida toodete turule laskmise ajal või tekkida tulenevalt tarkvarauuenditest või toote kasutamise kestel toimunud iseõppimisest. EL peaks täielikult ära kasutama oma käsutuses olevad vahendid, et täiendada oma tõenditebaasi tehisintellektiga seotud potentsiaalsete riskide kohta, sealhulgas kasutades tehisintellektist tulenevate ohtude kaardistamisel ELi Võrgu- ja Infoturbeameti (ENISA) kogemusi.

Nagu eespool märgitud, vaeb mitu liikmesriiki juba praegu võimalusi võtta tehisintellektist tingitud probleemide käsitlemiseks vastu siseriiklikke õigusakte. See tingib ühtse turu killustatuse riski. Tõenäoliselt loovad üksteisest lahknevad siseriiklikud õigusnormid takistusi ettevõtjatele, kes soovivad tehisintellektisüsteeme ühtsel turul müüa ja käitada. ELi tasandil tagatud ühine lähenemisviis võimaldab Euroopa äriühingutel saada hõlpsa juurdepääsu ühtsele turule ja toetab nende konkurentsivõimet üleilmsetel turgudel.

Aruanne selle kohta, milline on tehisintellekti, asjade interneti ja robootika mõju ohutusele ja vastutusele

Käesoleva valge raamatu juurde kuuluvas aruandes analüüsitakse asjaomast õigusraamistikku. Selles loetletakse nimetatud raamistiku kohaldamise ebakindlad aspektid seoses eririskidega tehisintellektisüsteemide ja muu digitehnoloogia puhul.

Aruande järeldus on, et kehtivates tooteohutusalastes õigusaktides kasutatakse juba praegu ohutuse laiendatud käsitust ja seega on tagatud kaitse igasuguste tootest tulenevate riskide eest vastavalt selle kasutamisele. Teisalt võidakse õiguskindluse suurendamiseks kehtestada sätted, mis käivad spetsiaalselt uute digitehnoloogiast johtuvate riskide kohta.

- Teatavate tehisintellektisüsteemide autonoomne tegutsemine nende elutsükli jooksul võib tuua kaasa olulised muutused toote juures, see aga mõjutab ohutust ja võib tingida uue riskihindamise vajaduse. Lisaks sellele on võimalik, et alates toodete projekteerimisest ning tehisintellektitoodete ja -süsteemide kogu elutsükli jooksul tuleb kaitseabinõuna kohaldada inimjärelevalvet.
- Vajaduse korral võiks kaaluda ka sõnaselgeid nõudeid tootjatele seoses riskidega vaimsele tervisele (näiteks koostöö puhul humanoidrobotitega).
- Liidu tooteohutusalastes õigusaktides võiksid olla sätestatud erinõuded, mis käsitleksid riske seoses ohutust puudutavate andmete ekslikkusega projekteerimisetapis, samuti mehhanismid, millega oleks tagatud andmete kvaliteedi säilimine tehisintellektitoodete ja -süsteemide kasutamisel.
- Algoritmipõhiste süsteemide läbipaistmatuse saaks neutraliseerida läbipaistvusnõuetega.
- Võimalik, et olemasolevaid norme on vaja kohandada ja selgitada juhul, kui turule lastakse autonoomne tarkvara või kui see laaditakse pärast selle turule laskmist tootesse ja kui see mõjutab turvalisust.
- Võttes arvesse uue tehnoloogia tarneahelate üha suuremat keerukust, saaks tarneahelasse kuuluvate majandustegevuses osalejate ja kasutajate vahelist koostööd nõudvate konkreetsete sätetega tagada õiguskindluse.

Sellise uue digitehnoloogia nagu tehisintellekt, asjade internet ja robootika omadused võivad muuta küsitavaks teatavad tootevastutusraamistike aspektid ja vähendada nende tulemuslikkust. Mõned neist omadustest võivad raskendada kahju seostamist isikuga, mis on vastavalt enamike riikide õigusnormidele vajalik süül põhineva kahjunõude esitamiseks. See võib oluliselt suurendada ohvrite kulu ja tähendab, et keerukas võib olla esitada või tõendada vastutusest tulenevaid nõudeid muude isikute vastu kui tootjad.

- Tehisintellektisüsteemide osaluse tõttu kahju kandnud isikutel peab olema samal tasemel kaitse nagu muu tehnoloogia tõttu kahju kandnud isikutel, samas kui tehnoloogilistel uuendustel peaks lubatama edasi areneda.
- Kõiki selle eesmärgi tagamise viise tuleks põhjalikult kaaluda, sealhulgas võimalikke muudatusi tootevastutuse direktiivis ja võimalust riiklike vastutust käsitlevate õigusnormide täiendavaks sihipäraseks harmoneerimiseks. Näiteks ootab komisjon seisukohti selle kohta, kas ja mil määral võib olla vajalik leevendada keerukuse tagajärgi, kohandades tõendamiskoormist, mis on riiklike vastavust käsitlevate õigusnormidega kehtestatud tehisintellektirakenduste kasutamisest tuleneva kahju puhul.

Komisjon järeldab eeltoodud arutelu põhjal, et lisaks võimalikele kohandustele kehtivates õigusaktides võib olla tarvis konkreetselt tehisintellekti käsitlevat õigusakti, et muuta ELi õigusraamistik vastavaks praegusele ja prognoositavale tehnoloogia ja kaubanduse arengule.

C. ELI TULEVASE ÕIGUSRAAMISTIKU KOHALDAMISALA

Keskne küsimus tulevase konkreetselt tehisintellekti käsitleva õigusraamistiku puhul on selle kohaldamisala määratlemine. Tööhüpotees on, et õigusraamistikku kohaldatakse tehisintellekti kasutavate toodete ja teenuste suhtes. Tehisintellekt tuleks seega nii käesoleva valge raamatu kui ka mistahes tulevase poliitilise algatuse otstarbel selgelt määratleda.

Komisjon määratles tehisintellekti esimest korda oma teatises „Tehisintellekt Euroopa huvides“[46]. Seda määratlust täpsustas kõrgetasemeline eksperdirühm[47].

Mis tahes uues õiguslikus vahendis sisalduv tehisintellekti definitsioon peab olema piisavalt paindlik, et võtta arvesse tehnika edusamme, ja samas piisavalt täpne, et tagada vajalik õiguskindlus.

Näiteks autonoomse sõidukijuhtimise puhul kasutab algoritm teavet, mida ta saab autost (kiirus, kütusekulu, amortisaatorid jne) ja auto ümbrust seiravatelt anduritelt (tee, liiklusmärgid, teised sõidukid, jalakäijad jne), et järeldada, millisesse suunda ning millise kiirenduse ja kiirusega auto peaks teatavasse sihtkohta jõudmiseks liikuma. Kogutud andmete põhjal kohandub algoritm teeolukorra ja välistingimuste, sealhulgas muude juhtide käitumisega, et saavutada võimalikult mugav ja turvaline teekond.

Käesoleva valge raamatu ja samuti kõigi tulevaste poliitilisi algatusi käsitlevate arutelude seisukohast tundub oluline määratleda selgelt tehisintellekti peamised koostisosad, see tähendab „andmed“ ja „algoritmid“. Tehisintellekti saab integreerida riistvarasse. Tehisintellekti alamkategooria moodustavate masinõppemeetodite puhul treenitakse algoritme tuletama andmestiku põhjal teatavaid kujundeid, et määrata kindlaks konkreetse eesmärgi saavutamiseks vajalikud toimingud. Algoritmid võivad kasutamise kestel õppimist jätkata. Ehkki tehisintellekti põhised tooted võivad tegutseda autonoomselt, tajudes oma ümbrust ja omamata eelnevalt kindlaks määratud juhiseid, määrab ja piirab nende käitumist suuresti nende arendaja. Inimesed määravad ja programmeerivad eesmärgid, mille saavutamiseks peaks tehisintellektisüsteem oma tegevuse optimeerima.

EL-il on olemas range õigusraamistik, et tagada muu hulgas tarbijakaitse, astuda vastu ebaausatele kaubandustavadele ning kaitsta isikuandmeid ja privaatsust. Lisaks sellele sisaldab liidu õigustik konkreetseid norme teatavate sektorite kohta (näiteks tervishoid ja transport). Need olemasolevad ELi õiguse sätted kehtivad seoses tehisintellektiga ka edaspidi, ehkki võimalik, et digiülemineku ja tehisintellekti kasutamise kajastamiseks on nimetatud raamistikku vaja ajakohastada (vt punkt B). Sellest tulenevalt on need aspektid, mida on juba reguleeritud kehtivate horisontaalsete või

[46] COM(2018) 237 final, lk 1: „Tehisintellekt iseloomustab intelligentselt käituvaid süsteeme, mis analüüsivad oma keskkonda ja sooritavad teataval määral iseseisvaid toiminguid, et saavutada konkreetseid eesmärke.
Tehisintellektil põhinevad süsteemid võivad olla ainult tarkvarapõhised ja tegutseda virtuaalmaailmas (nt häälele reageerivad virtuaalassistendid, kujutise analüüsi tarkvara, otsingumootorid, kõne- ja näotuvastussüsteemid) või olla paigaldatud riistvarasse (nt kõrgtehnoloogilised robotid, isejuhtivad autod, droonid või asjade interneti rakendused).“

[47] Kõrgetasemeline eksperdirühm „Tehisintellekti määratlus“, lk 8: „Tehisintellektisüsteemid on inimeste projekteeritud tarkvara- (ja võimalik, et ka riistvara-) süsteemid, mis neile seatud keerulise sihi puhul tegutsevad füüsilises või digitaalses mõõtmes, tajudes oma ümbrust andmeid hõivates, kogutud struktureeritud või struktureerimata andmeid interpreteerides, neis andmetest tuletatud teadmise üle arutledes või infot töödeldes, ja valivad konkreetse eesmärgi saavutamiseks optimaalse(d) toimingu(d). Tehisintellektisüsteemid võivad kas kasutada sümboolseid reegleid või õppida digitaalse mudeli põhjal; samuti suudavad nad oma käitumist kohandada, analüüsides nende eelnevate toimingute mõju keskkonnale.“

valdkondlike õigusaktidega – näiteks meditsiiniseadmete[48] ja transpordisüsteemide puhul – ka edaspidi hõlmatud nende õigusaktidega.

Põhimõtteliselt peaks tehisintellekti uus õigusraamistik tulemuslikult oma eesmärgid saavutama, olemata samas ülemäära piirav, et vältida ebaproportsionaalse koormuse tekitamist (eriti VKEdele). Komisjon on seisukohal, et tasakaalu leidmiseks peab ta kasutama riskipõhist lähenemisviisi.

Riskipõhine lähenemisviis on oluline reguleeriva sekkumise proportsionaalsuse tagamiseks. Kuid selleks on vaja selgeid kriteeriumeid, et teha vahet erinevatel tehisintellektirakendustel, eriti mis puudutab küsimust, kas teatav rakendus on kõrge riskitasemega või mitte[49]. Kõrge riskitasemega tehisintellektirakenduse määratlus peaks olema selge ja hõlpsasti mõistetav ning kehtima kõigi asjaomaste osalejate puhul. Aga isegi kui tehisintellektirakendus ei kvalifitseeru kõrge riskitasemega rakenduseks, kehtivad selle suhtes täielikult juba olemasolevad ELi õigusnormid.

Komisjon leiab, et arvestades sellega, mis on kaalul, tuleks kõik tehisintellektirakendused lugeda üldjuhul kõrge riskitasemega rakendusteks, võttes seejuures arvesse, kas märkimisväärne risk kaasneb nii sektori kui ka kavandatava kasutamisviisiga, ennekõike ohutuse, tarbija õiguste ja põhiõiguste seisukohast. Täpsemalt tuleks tehisintellektirakendus lugeda kõrge riskitasemega rakenduseks, kui see vastab korraga mõlemale järgmisele kriteeriumile.

- Esiteks kasutatakse tehisintellektirakendust sektoris, mille tavapärase tegevusega arvestades on ootuspärane, et võivad esineda märkimisväärsed riskid. Esimese kriteeriumiga tagatakse, et regulatiivne sekkumine keskendub valdkondadele, mille puhul riskide realiseerumist peetakse üldiselt kõige tõenäolisemaks. Uues õigusraamistikus tuleks esitada üksikasjalik ja ammendav loetelu hõlmatud sektoritest; nende seas oleksid näiteks tervishoid, transport, energeetikasektor ja mõned avaliku sektori osad[50]. Loetelu tuleks korrapäraselt läbi vaadata ja seda tuleks vajaduse korral muuta vastavalt praktikas toimuvale arengule.
- Teiseks kasutatakse tehisintellektirakendust kõnealuses sektoris viisil, mille puhul on tõenäolised märkimisväärsed riskid. Teine kriteerium kajastab tõdemust, et sugugi mitte igasuguse tehisintellekti kasutamisega valitud sektorites ei kaasne märkimisväärne risk. Näiteks võib tuua tervishoiu, mis võib üldjuhul olla asjakohane sektor, kuid viga haigla vastuvõtuaegade broneerimise süsteemis ei tingi harilikult nii olulisi riske, et need õigustaksid õiguslikku sekkumist. Teatava kasutuse riskitaseme hindamisel võiks aluseks võtta selle mõju asjaomastele isikutele. Näiteks võib tuua tehisintellektirakenduste kasutamine viisil, millel on üksikisiku või ettevõtte õiguste seisukohast õiguslikud või sellega samaväärselt olulised tagajärjed, mille tõttu esineb kehavigastuste tekitamise või surma põhjustamise, märkimisväärse varalise või mittevaralise kahju oht või mille tagajärgi füüsilised või juriidilised isikud ei saa mõistlikkuse piires vältida.

Nende kahe kumulatiivse kriteeriumi kohaldamine tagaks, et õigusraamistikul on konkreetne kohaldamisala ja et see tagab õiguskindluse. Uues tehisintellekti käsitlevas õigusraamistikus sätestatud kohustuslikud nõuded (vt allpool punkt D) kehtiksid ainult nende rakenduste suhtes, mis oleksid nende kahe kumulatiivse kriteeriumi alusel määratletud kõrge riskitasemega rakendustena.

[48] Näiteks on turvakaalutlused ja õiguslikud tagajärjed erinevad sõltuvalt sellest, kas tegu on tehisintellektisüsteemidega, mis annavad erialast meditsiinilist teavet arstidele, tehisintellektisüsteemidega, mis annavad meditsiinilist teavet otse patsiendile, või süsteemidega, mis sooritavad patsiendi kallal ise otse protseduure. Komisjon vaeb neid tervishoiusektorile ainuomaseid turvalisuse ja tootjavastutusega seotud probleeme.

[49] Vastavalt valdkonnale (näiteks tooteohutuse puhul) võivad ELi õigusaktide riskikategooriad siinkirjeldatust erineda.

[50] Avalik sektor võiks hõlmata selliseid valdkondi nagu varjupaigaküsimused, ränne, piirikontroll ja kohtusüsteem ning sotsiaalkindlustus- ja tööturuasutused.

Eeltoodust hoolimata võib esineda ka erijuhte, kui tehisintellektirakenduste kasutamist teataval eesmärgil tuleb kaalul olevate riskidega arvestades lugeda kõrge riskitasemega kasutamisviisiks sektorist sõltumata ning mille suhtes kohaldataks endiselt eespool nimetatud nõudeid[51]. Selle illustreerimiseks võib tuua järgmised näited.

- Tehisintellektirakenduste kasutamist värbamisprotsessides ja töötajate õigusi mõjutavates olukordades loetaks igal juhul kõrge riskitasemega kasutusviisiks, võttes arvesse, kui oluline on see üksikisiku jaoks ja ELi võrdse tööalase kohtlemise õigustiku seisukohast, ja seega kehtiksid alati eespool nimetatud nõuded. Kaaluda võiks ka muid konkreetseid kasutusviise, mis mõjutavad tarbijate õigusi.

- Tehisintellektirakenduste kasutamist biomeetrilise kaugtuvastuse[52] ja muu sekkuva jälgimise tehnoloogia jaoks loetaks igal juhul kõrge riskitasemega kasutusviisiks ning seega kehtiksid alati eespool nimetatud nõuded.

D. NÕUETE LIIGID

Tehisintellekti tulevase õigusraamistiku kavandamise juures tuleb otsustada, millist liiki õiguslikult kohustuslikud nõuded tuleb kehtestada asjaomastele osalistele. Neid nõudeid võidakse standarditega täpsustada. Nagu märgitud eespool punktis C ja lisaks juba olemasolevatele õigusaktidele kehtiksid need nõuded ainult kõrge riskitasemega tehisintellektirakenduste puhul ning tagaksid seega, et regulatiivne sekkumine on sihipärane ja proportsionaalne.

Võttes arvesse kõrgetasemelise eksperdirühma suuniseid ja eelnevas tekstis esitatut, võiksid kõrge riskitasemega tehisintellektirakendustele esitatavad nõuded koosneda järgmistest põhielementidest, mida on üksikasjalikumalt kirjeldatud alltoodud alapunktides:

- treenimisandmed;
- andmete ja teabe säilitamine;
- esitatav teave;
- stabiilsus ja täpsus;
- inimjärelevalve;
- konkreetsed nõuded teatavatele erilistele tehisintellektirakendustele, nagu biomeetrilise kaugtuvastuse jaoks kasutatavad rakendused.

Õiguskindluse tagamiseks täpsustatakse neid nõudeid täiendavalt, et anda selge lähtepunkt isikutele, kes peavad neid täitma.

a) Treenimisandmed

Tähtsam kui kunagi varem on edendada, tugevdada ja kaitsta ELi väärtusi ja norme, eriti õigusi, mille annavad kodanikele ELi õigusnormid. Kahtlemata tuleb neid jõupingutusi teha ka käesolevas dokumendis käsitletavate kõrge riskitasemega tehisintellektirakenduste puhul, mida ELis turustatakse ja kasutatakse.

[51] Tuleb rõhutada, et samuti võidakse kohaldada muid ELi õigusakte. Näiteks võidakse tarbijale mõeldud tootesse integreeritud tehisintellektirakenduse ohutuse suhtes kohaldada üldise tooteohutuse direktiivi.

[52] Biomeetrilist kaugtuvastust tuleb eristada biomeetrilisest autentimisest: viimane on turbeprotsess, mis kasutab indiviidi kordumatuid bioloogilisi omadusi, et kontrollida, kas ta on isik, kelle ta väidab enda olevat. Biomeetrilise kaugtuvastuse puhul toimub mitme isiku identiteedi tuvastamine biomeetriliste tunnuste (sõrmejäljed, näokujutis, vikerkest, veresoonte muster jne) alusel kaugmeetodil, avalikus ruumis ning pideval ja alalisel viisil, võrreldes neid andmebaasis säilitatavate andmetega.

Nagu eespool öeldud, andmeteta pole ka tehisintellekti. Paljude tehisintellektisüsteemide toimimine ning tegevus ja otsused, mis võivad neist oleneda, sõltuvad suuresti andmekogumitest, mida kasutades süsteeme on treenitud. Seega tuleks võtta meetmed, millega on võimalik tagada, et tehisintellektisüsteemide treenimiseks kasutatud andmete puhul on järgitud ELi väärtusi ja norme, eriti mis puudutab ohutust ning kehtivaid põhiõiguste kaitse norme. Kaaluda võiks järgmiste nõuete kehtestamist tehisintellektisüsteemide treenimiseks kasutatavatele andmekogumitele.

- Nõuded, mille eesmärk on anda piisav kindlus selle kohta, et tehisintellektile tuginevate toodete või teenuste hilisem kasutamine on ohutu, see tähendab vastab nõuetele, mis on sätestatud kohaldatavates ELi ohutusnormides (nii olemasolevates kui ka võimalikes täiendavates normides). Näiteks võivad need olla nõuded, millega tagatakse, et tehisintellektisüsteeme treenitakse selliste andmekogumitega, mis on piisavalt ulatuslikud ja hõlmavad kõiki asjakohaseid stsenaariume ohtlike olukordade vältimiseks.

- Nõuded võtta mõistlikud meetmed, mille eesmärk on tagada, et tehisintellektisüsteemide sellisel hilisemal kasutamisel ei ole keelatud diskrimineerimiseni viivad tulemused. Need nõuded võiksid ennekõike sisaldada kohustust kasutada andmekogumeid, mis on piisavalt representatiivsed, eriti selleks, et tagada kõigi sugu, etnilist päritolu ja muid keelatud diskrimineerimise võimalikke põhjuseid puudutavate asjakohaste aspektide kajastatus kõnealustes andmekogumites.

- Nõuded, mille eesmärk on tagada tehisintellekti kasutavate toodete ja teenuste kasutamisel privaatsuse ja isikuandmete nõuetekohane kaitse. Neid küsimusi reguleerivad oma kohaldamisala piires isikuandmete kaitse üldmäärus ja õiguskaitsedirektiiv.

b) Teabe ja andmete säilitamine

Võttes arvesse paljude tehisintellektisüsteemide keerukust ja läbipaistmatust ning asjaolu, et seetõttu võib olla raske kontrollida vastavust kohaldatavatele normidele ning tagada nende täitmine, on tarvis nõudeid, mis puudutavad teabe säilitamist algoritmide programmeerimise ja kõrge riskitasemega tehisintellektisüsteemide treenimiseks kasutatud andmete kohta ning teatavatel juhtudel ka andmete eneste säilitamist. Ennekõike võimaldavad need nõuded jõuda tehisintellekti potentsiaalselt problemaatilise tegevuse või otsuse algallikani ja seda kontrollida. See peaks lihtsustama järelevalvet ja normide täitmise tagamist, kuid peale selle võib see suurendada asjaomaste majandustegevuses osalejate stiimuleid arvestada varasest etapist peale vajadusega neid norme järgida.

Sel eesmärgil võiks õigusraamistikuga ette näha kohustuse säilitada järgmist.

- Täpne teave andmekogumi kohta, mis on kasutatud tehisintellektisüsteemide treenimiseks ja katsetamiseks, sealhulgas kogumi peamiste omaduste kirjeldus ja see, kuidas andmekogum valiti.

- Teatavatel põhjendatud juhtudel andmekogumid ise.

- Dokumendid, mis puudutavad programmeerimis-[53] ja treenimismeetodeid, protsesse ja tehnilisi vahendeid, mida on kasutatud tehisintellektisüsteemide ülesehituseks, katsetamiseks ja valideerimiseks – sealhulgas vajaduse korral ohutusega seotud dokumendid – ja

[53] Näiteks dokumendid algoritmide kohta, sealhulgas eesmärk, mille saavutamiseks tegevus optimeeritakse, milline kaal on antud teatavatele parameetritele algetapis jne.

dokumendid selle kohta, kuidas on välditud kallutatust, mis võiks tingida keelatud diskrimineerimise.

Teavet, dokumente ja – kui see on asjakohane – andmekogumeid tuleks säilitada piiratud mõistliku aja jooksul, et tagada asjaomaste õigusaktide tulemuslik täitmine. Tuleks võtta meetmeid, millega oleks tagatud nende kättesaadavaks tegemine taotluse alusel eelkõige pädevatele asutustele katsete või kontrolli eesmärgil. Vajaduse korral tuleks ette näha kord, millega oleks tagatud konfidentsiaalse teabe, näiteks ärisaladuste kaitse.

c) Teabe esitamine

Läbipaistvusnõuded ei kehti sugugi ainult eespool, punktis c käsitletud teabe säilitamise nõuete kontekstis. Selleks et saavutada soovitud eesmärgid, ennekõike propageerida tehisintellekti vastutustundlikku kasutamist, suurendada usaldust ja hõlbustada (vajaduse korral) kaebuse esitamist, tuleb ilmtingimata anda ennetavalt asjakohast teavet kõrge riskitasemega tehisintellektisüsteemide kasutamise kohta.

Seetõttu võiks kaaluda järgmisi nõudeid.

- Tagada, et tehisintellektisüsteemide võimaluste ja piiride kohta esitatakse selge teave, eriti mis puudutab süsteemide kavandatud kasutuseesmärki, tingimusi, mille puhul need peaksid toimima ettenähtud viisil, ja konkreetse eesmärgi saavutamisel eeldatavat täpsusastet. See teave on oluline ennekõike süsteemide juurutajate jaoks, ent sellest võib kasu olla ka pädevatel asutustel ja mõjutatud isikutel.

- Kodanikke tuleks eraldi selgelt teavitada, kui nad suhtlevad tehisintellektisüsteemi, mitte inimesega. Ehkki ELi andmekaitsenormid sisaldavad juba praegu teatavaid sellekohaseid sätteid,[54] võib eespool loetletud eesmärkide saavutamiseks olla vaja täiendavaid nõudeid. Sellisel juhul tuleks vältida tarbetut koormust. Niisiis ei ole sellist teavet vaja esitada näiteks juhul, kui kodanikul on kohe selge, et ta suhtleb tehisintellektisüsteemiga. Lisaks sellele on oluline, et esitatav teave oleks objektiivne, kokkuvõtlik ja hõlpsasti mõistetav. Teabe esitamise viis tuleks valida vastavalt selle esitamise kontekstile.

d) Stabiilsus ja täpsus

Tehisintellektisüsteemid – eriti kõrge riskitasemega rakendused – peavad olema tehniliselt stabiilsed ja täpsed, et olla usaldusväärsed. See tähendab, et sellised süsteemid tuleb välja töötada vastutustundlikult ning võtta juba eelnevalt asjakohasel viisil arvesse riske, mille need võivad põhjustada. Nende väljatöötamine ja toimimine peab tagama, et tehisintellektisüsteemid käituvad kavandatud usaldusväärsel viisil. Tuleks võtta kõik mõistlikud meetmed, et viia kahju tekkimise risk miinimumini.

Seetõttu võiks kaaluda järgmisi elemente.

- Nõuded, millega tagatakse, et tehisintellektisüsteemid on kõigis elutsükli etappides stabiilsed ja täpsed või vähemalt kajastavad õigesti oma täpsusastest.

- Nõuded, millega tagatakse tulemuste korratavus.

[54] Lisaks sellele peavad vastutavad töötajad vastavalt isikuandmete kaitse üldmääruse artikli 13 lõike 2 punktile f esitama isikuandmete saamise ajal andmesubjektile täiendava teabe automatiseeritud otsuste kohta ja teatava lisateabe, mis on vajalik õiglase ja läbipaistva töötlemise tagamiseks.

- Nõuded, millega tagatakse tehisintellektisüsteemide suutlikkus tulla kõigis elutsükli etappides adekvaatselt toime vigade või ebajärjepidevusega.

- Nõuded, millega tagatakse, et tehisintellektisüsteemid suudavad vastu panna nii avalikele rünnakutele kui ka varjatud katsetele andmeid või algoritme muuta ning et sellisel juhul võetakse leevendusmeetmeid.

e) Inimjärelevalve

Inimjärelevalve aitab tagada, et tehisintellekti süsteem ei kahjustaks inimeste sõltumatust ega põhjustaks muid kahjulikke mõjusid. Usaldusväärse, eetilise ja inimesekeskse tehisintellekti eesmärgi saavutamine on võimalik ainult juhul, kui kõrge riskitasemega tehisintellektirakenduste puhul tagatakse inimeste asjakohane sekkumine.

Ehkki need tehisintellektirakendused, mille jaoks kaalutakse käesolevas valges raamatus õiguslikku erikorda, loetakse kõik kõrge riskitasemega rakendusteks, võib erinevatel juhtudel vaja minna erinevat liiki ja erineva ulatusega inimjärelevalvet. Ennekõike sõltub see süsteemide kavandatud kasutusviisist ja mõjust, mis võib nende kasutamisel olla mõjutatud kodanikele ja juriidilistele isikutele. Samuti ei piira see isikuandmete kaitse üldmäärusest tulenevaid õigusi juhul, kui tehisintellektisüsteem töötleb isikuandmeid. Näiteks võib inimjärelevalve väljenduda järgmiselt (loetelu ei ole ammendav).

- Tehisintellektisüsteemi väljund jõustub ainult juhul, kui inimene on selle eelnevalt üle vaadanud ja kinnitanud (näiteks sotsiaalkindlustushüvitise taotluse saab tagasi lükata ainult inimene).

- Tehisintellektisüsteemi väljund jõustub kohe, ent pärast seda sekkub inimene (näiteks krediitkaarditaotluse tagasilükkamise otsuse võib teha tehisintellektisüsteem, kuid pärast seda peab olema võimalik inimesepoolne läbivaatamine).

- Tehisintellektisüsteemi üle tehakse selle toimimise kestel järelevalvet ning reaalajas on võimalik sekkuda ja see välja lülitada (näiteks on isejuhtival autol olemas seiskamisnupp või -protseduur, kui inimene otsustab, et auto ei toimi ohutult).

- Projekteerimisetapis kehtestatakse tehisintellektisüsteemi toimimise suhtes piirangud (näiteks isejuhtiv auto lakkab toimimast vähese nähtavuse tingimustes, kui andurite usaldusväärsus võib väheneda, või püsib teatavas konkreetses olukorras tema ees olevast sõidukist kindlal kaugusel).

f) Erinõuded biomeetrilise kaugtuvastuse puhul

Erilist riski seoses põhiõigustega[55] kujutab enesest biomeetriliste andmete kogumine ja kasutamine [56] kaugtuvastuseks [57] (näiteks kui võtta avalikes kohtades kasutusele näotuvastus). Sõltuvalt

[55] Näiteks seoses inimväärikusega. Samuti on näotuvastustehnoloogia kasutamise puhul põhiõigustega seotud kesksete probleemide seas õigus eraelu austamisele ja isikuandmete kaitse. Samuti võib sellel olla mõju seoses diskrimineerimiskeelu ja erirühmade, nagu laste, eakate ja puuetega isikute õigustega. Lisaks sellele ei tohi tehnoloogia kasutamine piirata väljendus-, ühinemis- ja kogunemisvabadust. Vaata „Facial recognition technology: fundamental rights considerations in the context of law enforcement“, https://fra.europa.eu/en/publication/2019/facial-recognition.

[56] Biomeetrilised andmed on määratletud kui „konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või

biomeetriliseks kaugtuvastuseks kasutatavate tehisintellektisüsteemide kasutuseesmärgist, -kontekstist ja -ulatusest võib sellise kasutamise mõju põhiõigustele varieeruda märkimisväärselt.

Kui välja arvata erijuhud, on ELi andmekaitsenormidega põhimõtteliselt keelatud töödelda füüsilise isiku kordumatuks tuvastamiseks kasutatavaid biomeetrilisi andmeid[58]. Täpsemalt võib selline töötlemine isikuandmete kaitse üldmääruse kohaselt toimuda ainult piiratud arvul põhjustel, mille hulgast peamised on olulise avaliku huviga seotud põhjused. Sellisel juhul peab töötlemine toimuma ELi või siseriikliku õiguse alusel, tingimusel et seejuures peetakse kinni proportsionaalsuse põhimõttest, austatakse isikuandmete kaitse õiguse olemust ja kohaldatakse sobilikke kaitsemeetmeid. Õiguskaitsedirektiivi kohaselt peab töötlemine olema rangelt vajalik, lubatud liidu või liikmesriigi õigusega ja selle puhul tuleb kohaldada asjakohaseid kaitsemeetmeid. Kuna igasugune biomeetriliste andmete töötlemine füüsilise isiku kordumatuks tuvastamiseks seostuks erandiga ELi õiguses sätestatud keelust, kohaldataks selle suhtes ELi põhiõiguste hartat.

Sellest tuleneb, et vastavalt praegustele ELi andmekaitsenormidele ja põhiõiguste hartale võib tehisintellekti kasutada biomeetriliseks tuvastamiseks ainult juhul, kui selline kasutamine on nõuetekohaselt põhjendatud ja proportsionaalne ning selle puhul kohaldatakse asjakohaseid kaitsemeetmeid.

Selleks et tegeleda võimalike ühiskondlike probleemidega, mis seonduvad tehisintellekti kasutamisega avalikes kohtades nimetatud eesmärgil, ja et vältida siseturu killustatust, algatab komisjon Euroopa tasandil ulatusliku arutelu selle üle, millised on sellist kasutamist õigustavad olukorrad (ja kas neid üldse on) ja millised võiksid olla ühised kaitsemeetmed.

E. ADRESSAADID

Mis puudutab selliste õiguslike nõuete adressaate, mida kohaldataks eespool nimetatud kõrge riskitasemega tehisintellektirakenduste suhtes, tuleb arvesse võtta kaht peamist aspekti.

Esiteks tekib küsimus, kuidas jagada kohustused asjaomaste majandustegevuses osalejate vahel. Tehisintellektisüsteemi elutsüklis on palju osalisi. Nende hulgas on arendaja, juurutaja (isik, kes kasutab tehisintellektiga varustatud toodet või teenust) ja teised (tootja, turustaja või importija, teenuseosutaja ning kutseline või eraviisiline kasutaja).

Komisjon on seisukohal, et tulevases õigusraamistikus tuleks iga kohustust kohaldada selle/nende osaleja/osalejate suhtes, kellel on parimad võimalused tegeleda potentsiaalsete riskidega. Näiteks tehisintellekti arendajad võivad küll olla kõige kohasemad tegelema arendusetapist tulenevate riskidega, kuid neil ei pruugi olla sama ulatuslikke võimalusi ohjata kasutusetapi riske. Sellisel juhul peaks vastav kohustus olema juurutajal. See ei mõjuta küsimust, milline osaleja peaks vastutama põhjustatud kahju eest, selleks et teha kindlaks vastutus lõppkasutajate või muude kahju kannatanud isikute ees ja tagada õiguskaitse tõhus kättesaadavus. Tootja vastutust käsitlevate ELi õigusnormide

---

kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed“ (õiguskaitsedirektiivi artikli 3 punkt 13; isikuandmete kaitse üldmääruse artikli 4 punkt 14; määruse (EL) 2018/1725 artikli 3 punkt 18).

[57] Näotuvastuse kontekstis tähendab tuvastamine seda, et isiku näokujutise malli võrreldakse paljude teiste andmebaasis säilitatavate mallidega, et teha kindlaks, kas seal säilitatakse tema kujutist. Teisalt autentimist (või kontrollimist) nimetatakse sageli üks-ühele tuvastusprotsessiks. See lubab võrrelda kaht biomeetrilist malli, mille puhul tavaliselt eeldatakse, et need kuuluvad ühele ja samale isikule. Kaht biomeetrilist malli võrreldakse selleks, et teha kindlaks, kas mõlemal kujutisel on sama inimene. Seda protseduuri kasutatakse näiteks automaatsetes piirikontrolliväravates, mida kasutatakse lennujaama piirikontrollis.

[58] Isikuandmete kaitse üldmääruse artikkel 9; õiguskaitsedirektiivi artikkel 10. Vt ka määruse (EL) 2018/1725 (kohaldatakse ELi institutsioonide ja organite suhtes) artiklit 10.

kohaselt vastutab puudusega toote eest tootja, ilma et see mõjutaks siseriiklikke õigusakte, millega võib olla lubatud nõude esitamine ka muudele isikutele.

Teiseks tekib küsimus õigusliku sekkumise geograafilise kohaldamisala kohta. Komisjoni arvates on ülimalt oluline, et nõuded kehtiksid kõigi asjaomaste majandustegevuses osalejate suhtes, kes pakuvad ELis tehisintellekti toetavaid tooteid või teenuseid sõltumata sellest, kas nad on asutatud ELis või mujal. Vastasel juhul ei oleks võimalik täielikult saavutada õigusliku sekkumise varem mainitud eesmärke.

F. ÕIGUSNORMIDE JÄRGIMINE JA NENDE TÄITMISE TAGAMINE

Tagamaks, et tehisintellekt on usaldusväärne ja turvaline ning kooskõlas Euroopa väärtuste ja normidega, tuleb kohaldatavaid õiguslikke nõudeid praktikas täita ning nii pädevad riiklikud asutused kui ka Euroopa asutused ja mõjutatud isikud peavad tagama nende tulemusliku täitmise. Pädevad asutused peaksid suutma uurida konkreetseid juhtumeid ja hinnata mõju ühiskonnale.

Komisjon leiab praeguses etapis, et võttes arvesse suurt riski, mida teatavad tehisintellektirakendused enesest kodanikele ja ühiskonnale kujutavad (vt eespool punkt A), on teatavate kõrge riskitasemega rakenduste suhtes kohaldatavate nõuete (vt eespool punkt D) täitmise kontrolliks ja tagamiseks vaja objektiivset eelnevat vastavushindamist. Eelnev vastavushindamine võiks hõlmata katse-, kontrolli või sertifitseerimismenetlusi [59]. Selle juurde võiks kuuluda algoritmide ja arendamisetapis kasutatud andmekogumite kontroll.

Kõrge riskitasemega tehisintellektirakenduste vastavushindamine peaks olema osa vastavushindamise mehhanismidest, mis on juba praegu olemas paljude ELi siseturule lastavate toodete jaoks. Kui kasutada ei saa ühtki sellist olemasolevat mehhanismi, võib olla vajalik luua samasugused mehhanismid, juhindudes headest tavadest ning võimalikust sidusrühmadelt ja Euroopa standardiorganisatsioonidelt saadud tagasisidest. Igasugune selline uus mehhanism peaks olema proportsionaalne ja mittediskrimineeriv ning selle puhul tuleks kasutada läbipaistvaid ja objektiivseid kriteeriume kooskõlas rahvusvaheliste kohustustega.

Eelneval vastavushindamisel põhineva süsteemi projekteerimise ja evitamise juures tuleks eriliselt arvesse võtta järgmist.

- Eelnev vastavushindamine ei pruugi olla sobilik kõigi eelnevalt nimetatud nõuete kontrolliks. Näiteks teabe esitamise nõude täitmist ei ole üldiselt kuigi lihtne sellise hindamise varal kontrollida.

- Eriliselt tuleks arvesse võtta võimalust, et teatavad tehisintellektisüsteemid arenevad ja õpivad kogemustest, mistõttu võib nende eluaja jooksul vaja olla süsteemi korduvat hindamist.

- Vajadus kontrollida treenimiseks kasutatud andmeid ning tehisintellektisüsteemide ülesehituseks, katsetamiseks ja valideerimiseks kasutatud programmeerimis- ja treenimismeetodeid ning protsesse ja tehnikat.

- Juhul kui vastavushindamine näitab, et tehisintellektisüsteem ei vasta nõuetele, mis käivad näiteks selle treenimiseks kasutatud andmete kohta, tuleb kindlakstehtud vajakajäämised

[59] Süsteem põhineks ELi vastavushindamismenetlustel (vt otsus 768/2008/EL või määrus (EL) 2019/881 (küberturvalisuse määrus)), võttes arvesse tehisintellekti eripärasid. Vt 2014. aasta sinine raamat ELi toote-eeskirjade rakendamise kohta.

parandada, näiteks treenides süsteemi ELis uuesti viisil, millega on tagatud vastavus kõigile kohaldatavatele nõuetele.

Vastavushindamine oleks kohustuslik kõigile sihtrühma kuuluvatele majandustegevuses osalejatele nende asutamise kohast sõltumata[60]. Selleks et piirata VKEdele langevat koormust, võidakse kaaluda tugistruktuuri loomist, muu hulgas digitaalse innovatsiooni keskuste kaudu. Lisaks sellele hõlbustaksid nõuete täitmist eeskirjad ja samuti spetsiaalsed veebipõhised vahendid.

Varasem vastavushindamine ei tohiks mõjutada riigi pädevate ametiasutuste poolset nõuetele vastavuse kontrolli ja hilisemat õigusnormide täitmise nõudmist. See kehtib kõrge riskitasemega tehisintellektirakenduste puhul, aga ka muude tehisintellektirakenduste puhul, mille suhtes kohaldatakse õiguslikke nõudeid, ehkki esimesena nimetatud rakenduste kõrgest riskitasemest tulenevalt võivad riigi pädevad asutused neile erilist tähelepanu pöörata. Järelkontrolli nõudeid peaks olema võimalik täita küllaldase dokumentatsiooniga asjaomase tehisintellektirakenduse kohta (vt eespool punkt E) ja kolmandatele isikutele, näiteks pädevatele asutustele antava võimalusega selliseid rakendusi katsetada, kui see on vajalik. See võib olla eriti oluline juhul, kui tekivad põhiõigustega seotud riskid, mis sõltuvad kontekstist. Selline järelevalve nõuetele vastavuse üle võiks olla osa alalisest turujärelevalvekorrast. Juhtimisega seotud aspekte vaetakse pikemalt alltoodud punktis H.

Lisaks sellele tuleks nii kõrge riskitasemega tehisintellektirakenduste kui ka muude tehisintellektirakenduste puhul tagada tehisintellektisüsteemidest negatiivselt mõjutatud isikutele tulemuslikud õiguskaitsevahendid. Vastutusküsimusi on pikemalt käsitletud käesoleva valge raamatu juurde kuuluvas aruandes ohutus- ja vastutusraamistiku kohta.

G. VABATAHTLIK MÄRGISTUS TEHISINTELLEKTISÜSTEEMIDELE, MILLEGA EI OLE SEOTUD SUURT RISKI

Selliste tehisintellektirakenduste puhul, mis ei kvalifitseeru kõrge riskitasemega rakendusteks (vt eespool punkt C) ja mille suhtes ei kehti seega eespool loetletud nõuded (vt eespool punktid D, E ja F), oleks üks võimalus luua lisaks kohaldatavatele õigusaktidele vabatahtlik märgistuskord.

Asjast huvitatud majandustegevuses osalejad, kelle suhtes ei kehti kohustuslikud nõuded, võiksid selle korra kohaselt otsustada, et nad alluvad vabatahtlikult kas neile nõuetele või konkreetsele sarnaste nõuete paketile, mis on loodud spetsiaalselt vabatahtliku korra jaoks. Asjaomastele majandustegevuses osalejatele antakse seejärel nende tehisintellektirakendustele mõeldud kvaliteedimärgis.

Vabatahtlik märgis võimaldaks seda kasutavatel majandustegevuses osalejatel anda märku oma tehisintellekti kasutavate toodete ja teenuste usaldusväärsusest. See lubaks kasutajatel hõlpsasti ära tunda tooted ja teenused, mis vastavad teatavatele objektiivsetele ja ELi-ülestele ühtlustatud kriteeriumidele, mis on rangemad kui harilikult kohaldatavad juriidilised kohustused. See suurendaks tehisintellektisüsteemide usaldusväärsust kasutajate silmis ja soodustaks tehnoloogia üldist kasutuselevõttu.

See variant eeldaks, et koostatakse uus õigusakt, milles on sätestatud vabatahtliku märgistuse raamistik selliste tehisintellektisüsteemide arendajatele ja/või juurutajatele, mida ei loeta kõrge riskitasemega süsteemideks. Märgisesüsteemis osalemine oleks küll vabatahtlik, kuid kui arendaja või juurutaja on otsustanud märgist kasutada, on nõuded siduvad. Eel- ja järelkontrolli kombinatsioon peaks tagama, et kõiki nõudeid täidetakse.

[60] Asjaomase juhtimisstruktuuri – sealhulgas vastavushindamist tegema määratud asutuste – suhtes vt allpool punkt H.

H. JUHTIMINE

Selleks et vältida vastutuse killustamist, suurendada liikmesriikide suutlikkust ja tagada, et Euroopa hangib endale järk-järgult tehisintellekti kasutavate toodete ja teenuste katsetamiseks ja sertifitseerimiseks vajaliku suutlikkuse, on vaja Euroopa tehisintellekti alast juhtimisstruktuuri riiklike pädevate asutuste koostööraamistiku vormis. Sellega seoses oleks tulus toetada riiklikke pädevaid asutusi, et neil oleks võimalik oma volitusi ellu viia tehisintellekti kasutamise puhul.

Euroopa juhtimisstruktuuril võiks olla hulk erinevaid ülesandeid: olla foorum, kus vahetatakse teavet ja häid tavasid, teha kindlaks uued suundumused ning anda nõu standardiseerimise ja sertifitseerimise kohta. See peaks aitama kaasa õigusraamistiku rakendamisele, muu hulgas esitades suuniseid, arvamusi ja ekspertteavet. Sel eesmärgil peaks see tuginema riiklike asutuste võrgustikule ning nii riikliku kui ka ELi tasandi valdkondlikele võrgustikele ja reguleerivatele asutustele. Lisaks sellele võiks komisjoni abistada alaline ekspertide komitee.

Juhtimisstruktuur peaks tagama sidusrühmade võimalikult suure osaluse. Raamistiku rakendamise ja edasiarendamise suhtes tuleks konsulteerida sidusrühmadega, nagu tarbijaorganisatsioonid, sotsiaalpartnerid, ettevõtted, teadlased ja kodanikuühiskonna organisatsioonid.

Võttes arvesse juba olemasolevaid struktuure finants-, farmaatsiatööstuse, lennunduse, meditsiiniseadmete, tarbijakaitse ja andmekaitse valdkonnas, ei tohiks kavandatud juhtimisstruktuur dubleerida olemasolevaid funktsioone. See peaks looma tihedad sidemed teiste ELi ja riikliku tasandi pädevate asutustega erinevates sektorites, et täiendada olemasolevaid ekspertteadmisi ning aidata olemasolevaid asutusi tehisintellektisüsteeme ning tehisintellektivalmidusega tooteid ja teenuseid kasutavate majandustegevuses osalejate kontrolli ja järelevalve juures.

Kui valitakse see variant, võiks vastavushindamise tegemise usaldada liikmesriikide määratud teavitatud asutuste hoolde. Katsekeskused peaksid võimaldama tehisintellektisüsteemide sõltumatut kontrolli ja hindamist kooskõlas eespool visandatud nõuetega. Sõltumatu hindamine suurendab usaldust ja tagab objektiivsuse. Samuti võiks see hõlbustada asjaomaste pädevate asutuste tööd.

ELil on suurepärased katse- ja hindamiskeskused ning ta peaks arendama oma suutlikkust ka tehisintellekti vallas. Kolmandates riikides asutatud majandustegevuses osalejad, kes soovivad tulla siseturule, võiksid kas kasutada ELis loodud määratud asutusi või – tingimusel et kolmandate riikidega on sõlmitud vastastikuse tunnustamise lepingud – kasutada kolmandate riikide asutusi, mille ülesanne on teha sellist hindamist.

Tehisintellektiga seonduv juhtimisstruktuur ja siinkohal käsitletav võimalik vastavushindamine ei mõjutaks ELi õiguse kohaseid volitusi ja ülesandeid, mis on asjaomastel pädevatel asutustel, kes tegelevad konkreetse sektori või konkreetse küsimusega (finantsvaldkond, farmaatsiatööstus, lennundus, andmekaitse, tarbijakaitse jne).

6. KOKKUVÕTE

Tehisintellekt on strateegiline tehnoloogia, millest kodanikel, ettevõtetel ja ühiskonnal tervikuna võib olla väga palju kasu, tingimusel et see on inimkeskne, eetiline ja kestlik ning kooskõlas põhiõiguste ja -väärtustega. Tehisintellekt võimaldab olulist tõhususe ja tootlikkuse kasvu, mis võib suurendada Euroopa tööstuse konkurentsivõimet ja parandada kodanike elujärge. Samuti võib sellest abi olla lahenduste leidmisel mõnedele kõige pakilisematele sotsiaalsetele probleemidele, mille hulgas on võitlus kliimamuutuste ja keskkonnaseisundi halvenemise vastu, kestlikkuse ja demograafiliste muutustega seotud probleemid, liidu demokraatia kaitse ning vajaduspõhine ja proportsionaalne võitlus kuritegevuse vastu.

Selleks et Euroopa saaks tehisintellekti pakutavad võimalused täielikult ära kasutada, peab ta edasi arendama ja tugevdama selleks vajalikku tööstuslikku ja tehnoloogilist suutlikkust. Vastavalt käesoleva dokumendi juurde kuuluvas Euroopa andmestrateegias esitatule on selleks samuti tarvis meetmeid, mille aitavad Euroopal saada üleilmseks andmekeskuseks.

Euroopa käsitus tehisintellektist on suunatud Euroopa innovatsioonisuutlikkuse edendamisele tehisintellekti vallas ning toetab eetilise ja usaldusväärse tehisintellekti väljatöötamist ja kasutuselevõttu kõikjal ELi majanduses. Tehisintellekt peaks töötama inimeste hüvanguks ja olema ühiskonna heaolu mootor.

Käesoleva valge raamatu ja selle juurde kuuluva aruandega, mis käsitleb ohutus- ja vastutusraamistikku, algatab komisjon ulatusliku konsulteerimise liikmesriikide kodanikuühiskonna, tööstus- ja akadeemiliste ringkondadega seoses konkreetsete ettepanekutega, mis puudutavad Euroopa käsitust tehisintellektist. Ettepankute hulka kuuluvad nii poliitikameetmed, millega soodustada investeeringuid teadusuuringutesse ja innovatsiooni, aidata kaasa oskuste arendamisele ning toetada tehisintellekti kasutuselevõttu VKEde poolt, kui ka ettepanekud tulevase õigusraamistiku peamiste elementide kohta. See konsulteerimine võimaldab pidada kõigi asjaomaste isikutega ulatuslikku dialoogi, mis annab komisjonile juhiseid järgmisteks sammudeks.

Komisjon palub esitada märkused valges raamatu esitatud ettepanekute kohta avaliku konsultatsiooni raames veebisaidil https://ec.europa.eu/info/consultations_et. Konsultatsioon on märkuste esitamiseks avatud kuni 19. maini 2020.

Tavapäraselt avaldab komisjon avaliku konsultatsiooni tulemusel saadud märkused. Samas on võimalik esitada taotlus märkuste osaliselt või täielikult konfidentsiaalsena käsitlemiseks. Sellisel juhul tuleb edastatava dokumendi esimesele leheküljele teha selge märge avaldamiskeelu kohta ja saata komisjonile märkuste mittekonfidentsiaalne versioon, mille ta võib avaldada.