TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Eraõiguse osakond

Polina Krimm

TEHISINTELLEKTI POOLT ISIKUANDMETE TÖÖTLEMISE VASTAVUS ISIKUANDMETE KAITSE ÜLDMÄÄRUSES SÄTESTATUD LÄBIPAISTVUSE ALUSPÕHIMÕTTELE

Magistritöö

Juhendaja

prof Aleksei Kelli

Tallinn

2021

SISUKORD

SISSEJUHATUS

Tehisintellekti (ingl *artificial intelligence*) kasutamine on saanud lahutamatuks osaks hulgaliste isikuandmete töötlemisel nii era- kui ka avalikus sektoris. Nüüdisajal kaasatakse erinevates valdkondades ja tööprotsessides aina rohkem tehisintellekti tehnoloogiat, mis annab suuremad võimalused ja laiapindsemad rakendusviisid isikuandmete töötlemisel. Isikuandmete töötlemise seaduspärasus on seejuures prevaleeriv küsimus, mida ei saa jätta juhuse hooleks. Euroopa Liidu isikuandmete kaitse üldmääruses (ingl *General Data Protection Regulation* ehk GDPR, edaspidi IKÜM või üldmäärus)[1] sätestatud nõuetega vastavus tuleb tagada mistahes isikuandmete töötlemise puhul.

Järjest enam on päevakorda tulnud isikuandmete korrektne töötlemine ja selle ulatuse küsimus ühiskonna igapäevaste toimingute osas. Isikuandmete kaitse üldmäärus kohaldub „vastutava töötleja või volitatud töötleja tegevuskoha tegevuse kontekstis toimuva isikuandmete nii automatiseeritud kui ka automatiseerimata töötlemise suhtes.“[2] Kuivõrd tehisintellekti näol on tegemist automatiseeritud töötlemise protsessiga, siis isikuandmete kaitse üldmäärusest tulenevad nõuded kehtivad ka tehisintellekti abil isikuandmete töötlemise suhtes.

Tehisintellektiga seonduvaid küsimusi hakati Eestis põhjalikumalt uurima 2018.aastal, millal koondusid Riigikantselei ja Majandus- ja Kommunikatsiooniministeeriumi vedamisel nii era- kui ka avaliku sektori esindajad ekspertrühma, mille ülesanneteks olid seaduseelnõude koostamine Eesti õigusruumi selguse tagamiseks ja vajaliku järelevalve korraldamiseks, tehisintellekti tegevuskava välja töötamine ning tehisintellekti kasutuselevõtmisest avalikkuse teavitamine.[3] Ekspertrühma ettepanekute pinnalt koostati 2019. aastal tegevuskava Eestis tehisintellekti kasutuselevõtu edendamiseks aastateks 2019-2021.[4] 2020.aastal on Justiitsministeerium ette valmistanud algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsuse, mis saab peale väljatöötamiskavatsusele saadud ekspertide ja osapoolte tagasiside esitamist eelnõude aluseks, mille raames esitatakse ettepanek eraldiseisva

[1] 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.5.2016, lk 1-88.
[2] *Ibidem.*
[3] Riigikantselei ja Majandus- ja Kommunikatsiooniministeerium. Eesti tehisintellekti kasutuselevõtu eksperdirühma aruanne. Mai 2019. Avalikult kättesaadav krattide projekti kodulehel: https://www.kratid.ee/ (19.04.2021).
[4] Majandus- ja Kommunikatsiooniministeerium. Eesti riiklik tehisintellekti alane tegevuskava 2019-2021. – https://www.mkm.ee/sites/default/files/eesti_kratikava_juuli2019.pdf (19.04.2021).

algoritmiliste süsteemide seaduse välja töötamiseks.[5] Euroopa Liidu tasandil valmistatakse samuti ette tehisintellekti regulatsiooni, nimelt 2020. aastal on Euroopa Komisjon teinud algatuse tehisintellekti nii eetiliste kui ka õiguslike nõuete avalikuks aruteluks, misjärel 2021. aasta aprilli lõpus avalikustati Euroopa Parlamendi ja Nõukogu määruse ettepanek, milles esitab Euroopa Komisjon tehisintellekti riske käsitleva tehisintellekti õigusraamistiku.[6] Eeltoodust lähtuvalt on viimastel aastatel tehisintellekti rakendamisest tulenevad õiguslikud probleemid teravdatud tähelepanu all nii siseriiklikul kui ka Euroopa Liidu tasandil.

Käesoleva magistritöö valguses on valitud teema aktuaalne peale avalikkuse keskendumuse ka põhjusel, et tehisintellekti tehnoloogial põhinev isikuandmete töötlemine on automatiseeritud protsess, sestap tõusetub küsimus selle protsessi läbipaistvuse tagamises eelkõige puhkudel, kus profiilanalüüsi koostamisel võivad tehisintellekti algoritmid jõuda oma otsustusprotsessi tulemusena otsuseni, mis saab kaasa tuua negatiivseid või ettenägematuid hinnanguid konkreetse isiku kohta. Euroopa Komisjoni poolt välja antud Valges Raamatus tehisintellekti kohta toonitati tehisintellekti läbipaistmatusest põhjustatud probleeme, milleks on raskendatav kontroll põhiõiguste kaitseks kehtestatud olemasolevate Euroopa Liidu õigusaktidega vastavuse üle, takistus tagada nende õigusaktide täitmise tulemuslikkust ja füüsilistel isikutel resultatiivse juurdepääsu puudumine õigusmõistmisele nende suhtes negatiivse mõjuga omavate otsuste puhul. Veelgi enam ei pruugi olla vahendeid kontrollimaks, kuidas jõuti tehisintellekti kaasamise abil tehtud üksikotsuseni, ega kuidas järgiti taolisel juhul asjakohaseid norme.[7] Võttes esile toodud põhjendused arvesse, võivad antud töös tehtud järeldused omada teatud kasutegurit edaspidistes tehisintellekti seonduvate õigusprobleemide lahendamisel.

Magistritöö uurimisprobleemiks on tehisintellekti läbipaistmatusest tulenev risk isiku kohta ebasoodsate ja ootamatute järelduste tegemiseks profiilanalüüsi koostamisel ja muude automatiseeritud otsuste vastuvõtmisel.

[5] Justiitsministeerium. Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus (edaspidi „Krati VTK“). 14.08.2020 - https://adr.rik.ee/jm/dokument/7458502 (19.04.2021).
[6] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, COM/2021/206 final. Brussels, 21.04.2021. – https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (24.04.2021).
[7] Euroopa Komisjon. Valge Raamat. Tehisintellekt: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast, COM/2020/65 final. Brüssel, 19.02.2020. – https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_et.pdf (27.03.2021).

Tehisintellekti algoritmid suudavad õpetada ennast ise. Viimane tähendab seda, et taolise õppimise protsessi käigus võivad algoritmi parameetrid muutuda, mistõttu sellisel juhul ei ole mingil hetkel võimalik selle algoritmi loojal või kogenenud informaatikul suuta tehisintellekti arvustusi või otsuseid selgitada.[8]

Seega tehisintellekti kaasamine isikuandmete töötlemisse protsessi võib viia olukorrani, kus arvukatest andmetest tuletab tehisintellekt profiilanalüüsi raames järelduse, mis võib isikule avaldada negatiivset mõju või tagajärgi. Sellest johtuvalt tõusetuvad probleemid nii isiku põhiõiguste kaitse tagamise osas kui ka tuletatud otsuse usaldusväärsuse ja õiguspärasuse kahtluse alla seadmise osas.

Magistritöö eesmärgiks on välja selgitada, mil määral tehisintellekti rakendamisel isikuandmete töötlemisel profiilanalüüsis on võimalk täita isikuandmete kaitse üldmääruses sätestatud läbipaistvuse põhimõtet; ning kindlaks määrata, millised õiguslikud nõuded ja meetmed tagavad piisaval määral tehisintellekti süsteemide kaasamise abil isikuandmete töötlemise läbipaistvust.

Tulenevalt magistritöö uurimisprobleemist ja eesmärkidest on püsitatud järgmised uurimisküsimused:

- Millised on kõige levinumad kasutusel olevad tehisintellekti süsteemid?
- Millisel määral on tehisintellekti läbipaistvuse nõue võrdne IKÜM-is sätestatud läbipaistvuse põhimõttega?
- Kas ja kuidas saab tagada tehisintellekti algoritmidel põhineva isikuandmete töötlemise läbipaistvus ilma selle tehnilisse protsessi inimese poolt sekkumata?
- Kas ainult tehisintellekti protsesside arusaamisest piisab, et tagada isikute põhiõiguste kaitse?
- Millistele nõuetele peab vastama tehisintellekti läbipaistvus isikuandmete töötlemisel tulevikuperspektiivis Euroopa Liidu ja Eesti õiguses?

Magistritöö on jagatud kaheks peatükiks. Töö esimese peatükis vaadeldakse isikuandmete kaitse üldist kontseptsiooni ja reguleerimise vajalikkust, mille juures tuleb Euroopa Liidu

[8] Vt Krati VTK, lk 4.

õiguse tasandil juhinduda IKÜM-is kehtestatud nõuetest. Seejärel keskendub autor tehisintellekti käsitusele ja olemusele, põgusalt tutvustatakse kõige levinumaid masinõppe algoritmide tehnikaid, kuivõrd automatiseeritud isikuandmete töötlemine põhineb masinõppe algoritmidel. Lähemalt sisustatakse töö keskpunktis olev tehisintellekti läbipaistvus ja määratletakse tehisintellekti läbipaistvuse nõue eesmärgil vastandada seejärel seda IKÜM-is sätestatud läbipaistvuse põhimõttele. Samas peatükis peatutakse ja selgitatakse profiilianalüüsi mõistel ja esitletakse selle praktilist kasutust. Tuues seejuures mõningaid näited, et järgnevalt analüüsida tehisintellektist tulenevaid riske profiilianalüüsi koostamisel ja võimalust neid maandada läbi tehisintellekti läbipaistvuse saavutamise.

Magistritöö teises peatükis käsitletakse tehisintellekti süsteemide täiendava reguleerimise vajadust, selle lähtekohta ning kavatsust nii Euroopa Liidu tasandil kui ka Eestis, mille eesmärgiks peaks olema tagada tehisintellekti süsteemidel põhinevate protsesside läbipaistvus. Eraldi tuuakse välja tehisintellekti regulatsiooni oodatavad mõjud ühiskonnale ja vaadeldakse, mil määral tehisintellekti regulatsiooniga kaasneb võimalik ülereguleerimine tulevikuperspektiivis ning selle vältimise võimalust.

Tagamaks eelnevalt mainitud uurimisprobleemi lahendamine, eesmärkide saavutamine ja uurimisküsimustele vastamine võimalikult põhistatud järelduste saamiseks, on magistritöös kasutatud kvalitatiivset ja analüütilist meetodit. Täpsemalt on magistritöö näol tegemist kvalitatiivse uurimusega, kuid eesmärkide saavutamiseks kasutab autor analüütilist meetodit. Kvalitatiivse meetodi kasutamine tuleneb vajadusest teoreetiliselt analüüsida IKÜM-i regulatsioonist johtuvat läbipaistvuse põhimõtet tehisintellekti läbipaistvuse kontekstis. Analüütilist meetodit on rakendatud tööks vajaliku kirjanduse uurimisel, mis hõlmab endast nii IKÜM-ist tulenevate mõistete ja tehisintellekti tehnilise poole sisustamist ja kirjeldamist.

Tehisintellekti käsitlevate peatükkide kirjutamisel lähtub autor eelkõige inglisekeelsetest erialakirjandusest ja teadusartiklitest. Inglisekeelsete allikate kasuks otsustamine on tingitud peamiselt asjaolust, et tehisintellektiga seonduvaid nii teoreetilisi kui ka õigusküsimusi käsitletakse põhjalikult inglise keeles avaldatud teadusartiklites ja -töödes.

Kuivõrd magistritöö teema on tihedalt seotud isikuandmete töötlemise ja samaaegselt ka andmekaitse valdkonnaga, on prevaleeruva tähtsusega Euroopa Liidu isikuandmete kaitse

üldmäärus, uurimaks kõnealuse üldmääruse valguses tehisintellekti läbipaistvuse vastavust läbipaistvuse aluspõhimõttele isikuandmete töötlemisel. Lisaks, analüüsi aluseks võetakse töös Justiitsministeeriumi väljatöötamise kavatsus algoritmiliste süsteemide mõjude reguleerimise kohta, Euroopa Komisjoni asjakohased suunised usaldusväärse tehisintellekti kohta ja Euroopa Andmekaitsenõukogu poolt moodustatud artikli 29 Euroopa sõltumatu töörühma suunised. Lisaks eelnevale, on magistritöö oluliseks allikaks 2021. aasta aprillis avalikustatud Euroopa Parlamendi ja Nõukogu kavandatav määrus, mis käsitleb laiapõhjaliselt tehisintellektist tulenevaid riske. Magistritöös võetakse arvesse ettepanekus sisalduvat regulatsiooni ning tehisintellekti süsteemide läbipaistvuse saavutamise lähtekohti.

Seoses tehisintellekti tehnoloogia kiire arengu, laialdaste rakendamise võimaluste ja ühtlasi igapäevaellu lõimumisega on paari aasta jooksul oluliselt suurenenud tähelepanu sellega kaasnevate õiguslike küsimustele, mistõttu Tartu Ülikooli õigusteaduskonna nii era- kui ka avalikus õiguses kirjutatud magistritööde hulgas leidub tehisintellekti temaatikat käsitlevaid ja selle õiguse kontekstis analüüsitavaid teadustöid.

Avalikus õiguses on tehisintellekti temaatikal Tartu Ülikooli magistrantide poolt analüüsitud näiteks tehisintellekti kasutamise võimalusi haldusmenetluses, milles sedastati, et haldusmenetluse tehisintellekti süsteemidel on haldusakti andmisel või üldiselt haldusmenetluses kasutamisel mitmeid eeliseid, eelkõige tagab see haldusorganite töö suuremat efektiivsust.[9] Eraõiguses käsitlevad tehisintellekti ja isikuandmete kaitsega seonduvad magistritööde uurimused masinnägemise ja masinõppe rakendamist Euroopa Liidu õiguses emotsioonituvastuse ja Eesti korrakaitse jälgimisseadmestike näitel[10] ning tehisintellekti läbipaistvust isikuandmete kaitse regulatsiooni ja ärisaladuse konfidentsiaalsusnõude vaatenurgalt.[11]

Tööde maht näitab kõrgendatud huvi kasvu tehisintellektist tulenevate õiguslike probleemide uurimise vastu ning eelduslikult oodata ka tulevikus põhjalikke teadustöid kõnealuses

[9] Lember, K. Tehisintellekti kasutamine haldusakti andmisel. Tartu 2019, lk 65. – https://dspace.ut.ee/handle/10062/64057 (02.04.2021).
[10] Kruuse, K. Privaatsuse ja isikuandmete kaitse masinnägemise ja masinõppe kasutusel Euroopa Liidu õiguses emotsioonituvastuse ja Eesti korrakaitse jälgimisseadmestike näitel. Tallinn 2019. - https://dspace.ut.ee/handle/10062/64059 (02.0.2021).
[11] Žuk, J. Ärisaladuse ja isikuandmete kaitse regulatsiooni interaktsioon tehisintellekti läbipaistvuse tagamisel. Tallinn 2019. - http://dspace.ut.ee/handle/10062/64755 (02.04.2021).

valdkonnas. Uute regulatsioonide kehtestamise järel tekib õiguslikke küsimusi veelgi, mille puhul on edasiste uuringute läbiviimine märkimisväärselt tähtis.

Magistritöö märksõnadeks on tehisintellekt, andmekaitse, isikuandmete töötlemine ja läbipaistvus.

1. TEHISINTELLEKTI SÜSTEEMI LÄBIPAISTVUS ISIKUANDMETE TÖÖTLEMISE

1.1. Isikuandmete kaitse kontseptsioon ja vajadus Euroopa Liidu õiguses

Isikuandmete kaitse on viimasel kümnendil tõusnud üheks tähtsaimaks teemaks, mis mõjutab meie igapäeva elu märkimisväärselt. Võib jääda mõistetamatuks, millistel põhjustel on vajalik laiapõhjaline tehisintellekti süsteemide regulatsioon. Põhiõigused, millega andmekaitse kokku puutub, võivad olla esmapilgul arusaamatud, kuid suurim seos on sel õigusele privaatsusele. Järgnevas alapeatükis selgitatakse lähemalt andmekaitse kehtivat kontseptsiooni, millesse järjest enam peavad mahtuma ja sellega kooskõlas olema ka tehisintellekti süsteemid.

Euroopa Liidu põhiõiguste harta[12] sätestab õiguse privaatsusele ja isikuandmete kaitse põhiõigustena. Euroopa Liidu põhiõiguste harta artiklite 7 ja 8 (1) kohaselt on igaühel õigus tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust austamisele, ning õigus oma isikuandmete kaitsele. Isikuandmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja isiku nõusolekul või muul õiguslikul alusel ning isikul on õigus tutvuda tema kohta kogutud andmetega ja vajadusel nõuda nende parandamist tulenevalt Euroopa Liidu põhiõiguste harta artiklist 8 (2). Ühtlasi peab kogu seda protsessi kontrollima sõltumatu asutus, mis on samuti sätestatud Euroopa Liidu põhiõiguste harta artiklis 8 (3). Eestis tegutseb isikuandmete töötlemisele kehtestatud nõuete täitmise üle teostava sõltumatu järelevalveasutusena Andmekaitse Inspektsioon, mille pädevus ja ülesannete ulatus on sätestatud isikuandmete kaitse seaduses (edaspidi IKS).[13]

Privaatsuse defineerimine pole lihtne ülesanne. Privaatsuse kontseptsioonile on ette heidetud mitmeid tunnuseid: privaatsus on ärritavalt ebamäärane ja hääbuv, kurikuulsalt paindlik ja samas ühemõtteline, see hõlmab erinevaid ja eristatavaid tähendusi, kõrgelt subjektiivne, suhteline tulenevalt kultuurilisest taustast. Sellegipoolest, antud ebamäärasus ei vähenda

[12] Euroopa Liidu põhiõiguste harta – ELT C 326/391, 26.10.2012.
[13] Isikuandmete kaitse seadus – RT I, 04.01.2019, 11.

privaatsuse tähtsust.[14] Teisalt on isikute õigus privaatsusele saanud pidepunktiks nüüdisaegse isikuandmete kaitse kontseptsioonile ja informatsioonilise enesemääramise õiguseks.[15]

Andmekaitse on sarnaselt privaatsusele esmapilgul kaugel üheselt arusaadavast mõistest. Seda on keeruline defineerida mõne lausega, vaid andmekaitse üritab endas hõlmata seeriat ideedest, mis seostuvad isikuandmete töötlemisega.[16] Andmekaitse kontseptsiooni mõistmiseks on põhikohal töötlemine ja isikuandmed. Andmete töötlemist saab vaadata kui mistahes tegevust, mis algab nende kogumisest, salvestamisest, varundamisest ja kasutamisest, ja lõpeb nende avalikustamise, levitamise, kustutamise ning hävitamisega. Need muutuvad isikuandmeteks juhul, kui need on seostatavad mõne kindla füüsilise isikuga, keda nimetatakse ka andmesubjektiks.[17]

Lähenemisviisid andmekaitsele võivad olla erinevad, olenevalt, millisest eesmärgist või väärtusest lähtuda. Majanduse vaatenurgast on tähtis, et andmed ning informatsioon, mis võib endas sisaldada isikuandmeid, liiguks riikide vahel suuremate probleemideta. Sellest tulenevalt tuleb tagada, et isikuandmete kaitse ei tekitas juurde barjääre, mis piiraksid andmete vaba liikumist ja sellega takistaks majanduslikku arengut. Isikuandmete kaitse harmoniseerimine sellisel juhul edendaks andmevahetust ja läbi selle panustaks rahvusvahelise majanduse arengusse.[18]

Kõige terviklikum andmekaitse teooria on välja töötatud Paul de Herti ja Serge Gurwirthi poolt. Nende teooria arutleb erinevate rollide üle, mida privaatsus ja andmekaitse mängivad demokraatlikus riigis. Teooria aluseks on eeldus, et privaatsust ja andmekaitset saab vaadelda kui kaht eristatavat õiguslikku tööriista riigivõimu kontrollimiseks, mis täidavad erinevaid, kui üksteist toetavaid funktsioone. Privaatsust selles võtmes peetakse läbipaistmatuse tööriistaks ja andmekaitset vastupidiselt läbipaistvuse omaks.[19] Konstitutsioonilise demokraatliku riigi põhitunnuseks on areng, mis tuleneb isikute vabadusest. Privaatsfäär peab seega olema

[14] Tzanou, M. The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Oxford-Portland: Hart Publishing 2017, lk 7-8.
[15] Eneken, T. Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007, lk 72.
[16] Tzanou, lk 12.
[17] *Ibidem*, lk 12-13.
[18] *Ibidem*, lk 14-16.
[19] *Ibidem*, lk 32.

privilegeeritud vabaduste tagamise suunas ja selle tähtust ei saa alahinnata.[20] Sellest tulenevalt privaatsus üritab kaitsta inimesi võimu ebaseadusliku ja ülemäärase kasutamise vastu, kuid andmekaitse peaks kontrollima ning suunama seadusliku võimu kasutamist.[21]

Kokkuvõtvalt, andmekaitset saab pidada nii majanduse arengu kui ka põhiõiguste kaitsest lähtuvalt üheks tähtsaimaks tööriistaks. Informatsiooniajastul on vajalik tagada andmete, sh isikuandmete, vaba liikumine riikide ja jurisdiktsioonide vahel, kuid selle saavutamiseks ja võimalikke kaheti mõistetavuste vältimiseks on vajalik tagada ühine arusaam selle eesmärkidest ja kaitse vajadusest.

Andmekaitse standardid on viimastel aastatel saavutamas aina kõrgemat taset ja sellest tulenevalt on erinevad asutused valikute ees, kas nende andmete töötlemise protsessid on regulatsiooniga kooskõlas, eriti kui arvestada rahvusvahelist konteksti. Andmetel on võrratu omadus ületada piire ja mängida suurt rolli ülemaailmses digitaalses majanduses. Andmed on muutunud väärtuslikuks varaks ja neid lausa nimetatakse tuleviku valuutaks. Isikuandmete töötlemine saab toimuda läbi erinevate majandussfääride ja sotsiaalsete tegevuste ning infotehnoloogiliste vahendite arengu kaudu on muutunud isikuandmete töötlemine ja nende vahetus erinevate partnerite vahel aina lihtsamaks. Sellest kõigest lähtuvalt võttis Euroopa Liit vastu isikuandmete kaitse üldmääruse, harmoniseerimaks isikuandmete kaitse reegleid Euroopa Liidu liikmesriikide vahel ja tagamaks puudutatud inimeste õigust privaatsusele.[22]

Liikmesriikide õiguse harmoniseerimist võib pidada üheks põhiliseks IKÜM-i eesmärgiks. Samale eesmärgile oli suunatud ka 1995. aasta oktoobris rakendatud Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ (edaspidi isikuandmete kaitse direktiiv).[23] Isikuandmete kaitse direktiivi artikkel 1 lõiked 1 ja 2 sedastavad, et vastavalt direktiivile kaitsevad liikmesriigid isikuandmete töötlemisel füüsiliste isikute põhiõigusi ja -vabadusi ning eelkõige nende õigust eraelu puutumatusele, sealjuures ei tohtinud liikmesriigid piirata ega keelata isikuandmete vaba liikumist liikmesriikide vahel põhjusega, mis on seotud füüsilise isiku põhiõiguste ja -vabaduste

[20] De Hert, P. Gutwirth, S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy and the Criminal Law. Antwerpen-Oxford: Intersentia 2006, lk 70.
[21] Tzanou, lk 32.
[22] Voigt, P. Von dem Bussche, A. The EU General Data Protection Regulation (GDPR). A Practical Guide. Cham: Springer International Publishing 2017, lk 1.
[23] 24.oktoobri 1995.aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta - ELT L 281, lk 0031 – 0050.

kaitsega. Tulenevalt direktiivi olemusest, ei olnud selles toodud reegleid otsekohalduvad ja liikmesriigid pidid need enda seadusandlusesse üle võtma. Kuigi liikmesriigid võtsid direktiivi regulatsiooni samaväärselt üle, tekkisid liikmesriikide vahel märkimisväärsed erinevused selle tõlgendamise ja rakendamise osas. See viis üheselt olukorrani, kus isikuandmete kaitse määr ja ulatus erinesid riikide vahel märgatavalt.[24]

Eriti puudutas taoline regulatsioonide erinevus eraõiguslike juriidiliste isikute tegevust, mis omasid majandustegevust mitmes liikmesriigis, kus nad pidid täitma vastava riigi nõudeid ja praktikat. Sarnaselt tekitas see ebaselgust andmesubjektides, kelle õigusi võidi kaitsta ühes liikmesriigis laiemalt kui teises ning see viis kaugemale direktiivi eesmärkide saavutamine ja tagamine.[25] Otsekohaldatav määrus pidi suuremal määral välistama taolist ebaselgust, mis tuleneb regulatsiooni erinevast arusaadavusest ja tõlgendamisest liikmesriikide vahel.[26]

Isikuandmete kaitse üldmääruse üheks eesmärgiks on sammupidamine tehnoloogilise arenguga ja selle kaudu tulenevatest uutest ja teadmata riskidest. Infotehnoloogiline areng on andnud nii eraõiguslikele juriidilistele isikute kui ka avaliku võimu kandjatele võimalusele töödelda isikuandmeid järjest suuremal ja mõnedel juhtudel lausa hoomamata määral. Andmesubjektid avaldavad järjest enam enda isikuandmeid vabatahtlikult ja globaalsel skaalal.[27] Levinumateks vahenditeks taolise avaldamise jaoks on erinevad sotsiaalmeedia platvormid. Isikuandmete avaldamine on muutunud sotsiaalse elu osaks.

Murekohaks võib pidada asjaolu, et andmesubjektid ei oma piisavat kontrolli enda isikuandmete üle ja kartus, et nad ei suuda enda õigusi efektiivselt kaitsta. Isikuandmete töötlemine kasutades selleks internetist tulenevaid võimalusi on muutnud taolise töötlemise veel enam arusaadamatuks ja aina keerulisemaks näha riske, mis töötlemisega võivad kaasneda. IKÜM eesmärgiks on seega andmesubjekti õiguste tugevdamine ja usalduse taastamine andmesubjekti ja töötlevate ettevõtete vahel, näitamaks töötlemist selle seaduslikkuse eesmärgist.[28]

[24] Rücker, D. Kugler, T. New European General Data Protection Regulation. A Practitioner's Guide. Baden-Baden: Nomos Verlagsgesellschaft 2018, lk 1-2.
[25] *Ibidem*, lk 2.
[26] *Ibidem.*
[27] *Ibidem*, lk 3.
[28] *Ibidem.*

Sarnaselt isikuandmete kaitse direktiivile on IKÜM artikkel 1 lõikes 3 toodud põhimõte, et „isikuandmete vaba liikumist liidus ei piirata ega keelata põhjustel, mis on seotud füüsiliste isikute kaitsega isikuandmete töötlemisel.“ Sellega seab IKÜM eesmärgiks isikuandmete vaba liikumise, panustades sellega vabaduse, turvalisuse, õigluse ning vaba majandusühenduse loomisesse, tagamaks majandusliku ja sotsiaalse võrdväärse arengu tugevdamaks ühisturgu ja füüsiliste isikute heaolu.[29] Samuti peaks määrus tagama olukorra, kus ettevõtted omavad kokkupuudet vaid ühe järelevalveasutusega, muutes äritegevuse Euroopa Liidus lihtsamaks ja odavamaks.[30]

Eeltoodust tulenevalt on üldmäärus seadnud eesmärgiks isikuandmete tõhusama kaitse, kaasates sellesse kõikvõimalikud platvormid ja tulevikuperspektiivid ning harmoniseerides selles vallas Euroopa Liidu liikmesriikide õiguslikke regulatsioone. Tähelepanuta ei saa jätta isikuandmete vaba liikumise tagamist, millele toetub Euroopa majanduslik vabadus ja ühisturu efektiivne toimimine.

Sisulise kohaldamisala mõistes IKÜM kehtib, st „kohaldatakse isikuandmete täielikul või osalisel automatiseeritud töötlemise suhtes ja isikuandmete automatiseerimata töötlemise suhtes, kui kõnealused isikuandmed kuuluvad andmete kogumisse või kui need kavatsetakse andmete kogumisse kanda“ tulenevalt IKÜM artikli 2 lõikest 1. Sisuliselt ei kohaldata määrust IKÜM artikli 2 lõikel 2 rajanevalt juhtudel, mil „isikuandmeid töödeldakse muu kui liidu õiguse kohaldamisalasse kuuluva tegevuse käigus, mil liikmesriigid töötlevad isikuandmeid sellise tegevuse käigus, mis kuulub ühise välis- ja julgeolekupoliitika kohta, mil isikuandmeid töötleb füüsiline isik eranditult isiklike või koduste tegevuste käigus, või mil isikuandmeid töötlevad pädevad asutused süütegude tõkestamise, uurimise, avastamise või nende eest vastutusele võtmise ja kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil.“

Lisaks sisulisele kohaldamisalale, IKÜM artikli 3 lõike 1 kohaselt kohaldub määrus territoriaalselt „liidus asuva vastutava töötleja või volitatud töötleja tegevuskoha tegevuse kontekstis toimuva isikuandmete töötlemise suhtes sõltumata sellest, kas töödeldakse liidus või väljaspool liitu.“ Tulenevalt IKÜM artikli 3 lõikest 2 kohaldatakse määrust liidus asuvate

[29] Rücker/Kugler, lk 3-4.
[30] *Ibidem*, lk 4.

andmesubjektide töötlemise suhtes mujal kui liidus asuva vastutava töötleja või volitatud töötleja poolt, kui andmete töötlemine on seotud nende andmesubjektidele kaupade või teenuste pakkumisega olenemata tasu maksmisest, ning juhtudel, kui jälgitakse andmesubjektide tegevust, kui vastav tegevus toimub liidus. Samuti leiab määrus kohaldamist IKÜM artikli 3 kõike 3 järgi „isikuandmete töötlemise suhtes vastutava töötleja poolt, kelle asukoht ei ole liidus, vaid kohas, kus rahvusvahelise avaliku õiguse kohaselt kohaldatakse mõne liikmesriigi õigust."

Sisulisest kohaldamisalast välja jäävad seega olukorrad, kus ei toimu automatiseeritud töötlemist ning automatiseerimata töötlemine ei ületa teatavat strukturaalset lävendit ja seega ei kanna endast suurt riski isikuandmete töötlemisel. Samas tuleb taolist töötlemist pidada pigem erandlikuks ja juriidiline isik peaks eelkõige lähtuma, et igasugune temapoolne isikuandmete töötlemine langeb IKÜM kohaldamisalasse.[31] Teiseks suuremaks erandiks on isikuandmete töötlemine füüsilise isiku poolt eranditult isiklike või koduste tegevuste käigus. Sellega jääb määruse kohaldamisalast välja isikuandmete töötlemine, kui füüsiline isik teeb seda väljaspool ametialast või äritegevust. „Isiklik või kodune tegevus võib hõlmata kirjavahetust ja aadresside loetelu või tegevust suhtlusvõrgustikes ja Internetis. Erand ei välista määruse kohaldamist vastutavate töötlejate või volitatud töötlejate suhtes, kes pakuvad isikuandmete isiklikel või kodustel eesmärkidel töötlemise vahendeid."[32]

IKÜM artikli 4 punkti 1 mõistes defineeritakse isikuandmeid kui igasugust teavet tuvastatud või tuvastatava füüsilise isiku kohta. Seega saab isikuandmete definitsioonist tuvastada nelja erinevat elementi. Esimeseks on „igasugune teave", mis enda tähendusest tulenevalt viitab soovile laiendatult tõlgendada teavet, mis isikuandmete alla võib kuuluda. Igasugune teave hõlmab endast kõike, mida on võimalik füüsilise isiku kohta väita, olgu see tõde või vale.[33] Vastava teabe lai tõlgendus on kinnitust leidnud Euroopa Kohtu praktikas, et isikuandmete alla kuuluvad kindlasti isiku nimi koos tema telefoninumbrite või teabega tema töötingimuste või vaba aja harrastuste kohta.[34]

[31] Rücker/Kugler, lk 12.
[32] IKÜM, põhjendus 18.
[33] Rücker/Kugler, lk 13.
[34] EK C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596, p 24.

Järgmiseks kohustuslikuks elemendiks on teabe seotus füüsilise isikuga põhimõttelisel alusel. Teabe seotus võib tuleneda kolmest alternatiivsest aspektist. Sisu poolest on teave indiviidiga seotud just sellistel juhtudel, kui teave on sellest konkreetsest isikust. Näiteks on sellise teabega kindlasti tegemist patsiendi kohta käiva terviseanalüüsi osas või mõne ettevõtte teabekogumis olev kaust, mis on seotud konkreetse kliendiga ja sisaldab infot selle konkreetse kliendi kohta.[35] Eesmärgi element on täidetud, kui teavet kasutatakse või seda on võimalik kasutada kindlal eesmärgil hinnata, kohelda kindlaks määratud viisil või mõjutada indiviidi käitumist või tema staatust. Näiteks isiku kõnelogi annab võimaluse hinnata töötaja käitumist või tegevusi tema töökohal ja teha sellest vajalikke järeldusi.[36] Tulemuse või tagajärje element on täidetud juhtudel, kui teabe kasutamine avaldab suure tõenäosusega mõju kindla isiku õigustele või huvidele. Näiteks on jälgides taksoteenuse kvaliteedi parandamise huvides taksode asukohti ja marsruute, on võimalik teha järeldusi ka taksojuhtide käitumisele ehk nende töötamist ja selle efektiivsust.[37] Teabe seotus isikuga võib olla otsene või kaudne. Kaudselt võib tunduda, et teave on seotud mitte andmesubjektiga vaid mõne objektiga, kuid sellest on võimalik teha järeldusi isiku suhtes. Näiteks kinnisvara väärtus on otseselt seotud vaid konkreetse kinnisasjaga, kuid teades kinnisasja omanikku, saab kaudselt teha järeldusi isiku kohta, nt tema sissetulek või isegi maksukohustused, mis kinnisasjaga kaasnevad.[38]

Järgmine kohustuslik element isikuandmete puhul on andmesubjekti tuvastus. Tulenevalt üldmääruse artikli 4 punktist 1 peab isik olema teabes tuvastatud või vähemalt tuvastatav. Andmesubjekti ei peeta tuvastatavaks, kui tema tuvastamiseks tuleks teha ebamõistlikult palju aega, vaeva ja ressursse nõudvaid toiminguid.[39] Vastavalt IKÜM artikli 4 punktile 1 on füüsiline isik tuvastatav, kui teda saab „tuvastada otseselt või kaudselt, eelkõige taolise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator (IP-aadress) või füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal.“ Isikuandmetena on võrguidentifikaator eelkõige käsitatav juhtudel kui esinevad seaduslikud vahendid, mis võimaldavad elektrooniliste teabe- ja sideteenuste pakkujal pöörduda eelkõige küberrünnete korral pädeva asutuse poole, et see teeks vajalikud toimingud, et saada internetiühenduse

[35] Rücker/Kugler, lk 15.
[36] *Ibidem.*
[37] *Ibidem,* 15-16.
[38] *Ibidem*, lk 16.
[39] European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018, lk 92-93. – https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (11.04.2021).

pakkujalt andmeid, mille kaudu on võimalik tuvastada konkreetne isik, kes on seotud kindla võrguidentifikaatoriga.[40]

Viimasena on kohustuslikuks elemendiks elus olev füüsiline isik ise. Tulenedes selles, et just elus oleval füüsilisel isikul on õigus eraelu puutumatusele e privaatsusele. Surnud isikud on jääavad eelduslikult määruse kohaldamisalast välja, kuid võivad muudel põhjustel siiski sinna kuuluda. Sellisteks põhjusteks võivad olla erinevad asjaolud. Liikmesriigid võivad surnud isikute puhul ise täiendavaid reegleid kehtestada. Andmete töötlemisel võib olla praktiliselt keeruline või lausa võimatu tuvastada, kas isik on elus või surnud, mille tõttu on lihtsam töödelda isikuandmeid ühtse kogumina. Surnute isikuandmetele võivad kehtida muud reeglid, mis pole seotud otseselt andmekaitsega, vaid näiteks keelatuks on isiku au teotamine. Samuti võib surnu isikuandmed kaudselt viidata elava andmesubjekti kohta käivale teabele.[41]

Määruse kaitse peaks rakenduma ainult füüsiliste isikute andmetele, olenemata nende kodakondsusest või elukohast. Juriidiliste isikute andmeid, sealjuures juriidilise isiku nime ja vormi ning kontaktandmeid määrus kaitsema ei peaks.[42] Sarnaselt surnud füüsiliste isikute andmetega, võivad määrusest tuleneva kaitse faktiliselt saada ka juriidilise isiku andmed, kui neid töödeldakse samades andmekogudes. Sellistel juhtudel on töötlejal lihtsam rakendada samasuguseid kaitsemeetmeid kõikidele.[43]

Isikuandmete kaitse üldmääruse nõudeid tuleb täita eelkõige füüsiliste isikute andmete automatiseeritud töötlemisel. Isikuandmete olemus pole alati iseenesest mõistetav ja tõlgendada tuleb neid vajadusel laiendatult.

[40] EK C-582/14, *Patrick Breyer versus Saksamaa Liitvabariik*, ECLI:EU:C:2016:779, p-d 47-49.
[41] Rücker/Kugler, lk 21-22.
[42] IKÜM, põhjendus 14.
[43] Rücker/Kugler, lk 22.

1.2. Tehisintellekti määratlus ja masinõppe tehnikad

Mõistagi tuleb tehisintellekti tehnoloogiast arusaamiseks kindlaks määrata, mida tehisintellekt endast kujutab. Vaatamata sellele, et tehisintellekti puhul ei ole tegemist uue nähtusega, ei ole tehisintellekti mõiste ja selle olemuse ühist ja laialdaselt tunnustatud doktriinilist käsitlust siiani välja töötanud.[44]

Ehkki tehisintellekti mõistet defineeritakse erinevalt, need mõisted määratletakse kahe peamise dimensiooni järgi – esimene on seotud mõtteprotsessi (ingl *thought processes*) ja arutluskäiguga (ingl *reasoning*) ning teine on suunatud käitumisele (ingl *behaviour*). Mõtteprotsessi ja arutluskäiguga seonduvad definitsioonid mõõdavad edukust inimese võimekuse seisukohalt, käitumisele suunatud definitsioonid aga ideaalse intellekti kontseptsiooni vastu, mida nimetakse ratsionaalsuseks. Inimesekeskne lähenemine jaotub süsteeme inimesena mõtlevaks ja inimesena käituvaks, ratsionalistlik lähenemine aga ratsionaalselt mõtlevaks ja ratsionaalselt käituvaks süsteemideks, mida on ajalooliselt järgitud ning andnud väärtuslikke tulemusi.[45]

Euroopa Komisjon defineerib tehisintellekti kui tarkvarapõhiseid ja virtuaalmaailmas tegutsevaid või paigaldatud riistvarasse süsteeme, mis käituvad intelligentselt, analüüsivad ümbruskonda ja teostavad teatavas ulatuses iseseisvaid toiminguid konkreetsete eesmärkide saavutamiseks.[46] Eesti keele seletavast sõnaraamatust leidub kaks tehisintellekti definitsiooni: „modelleeritud ajuprotsessidest tulenev arvuti suutlikkus jäljendada inimese vaimset tegevust, tehisaru“ ja „arvutiteaduse ja -tehnika haru, mis uurib ajuprotsesside modelleerimist elektronarvutil ja vastavate arvutisüsteemide loomise meetodeid“.[47] Käesolevas töös ei keskendata tehisintellektile kui teadusharule, kuivõrd vastamaks seatud uurimisküsimustele käsitletakse tehisintellekt süsteemina, mida iseloomustavad teatud tunnused. Tartu Ülikooli

[44] Begishev, I. Latypova E. Kirpichnikov, D. Artificial Intelligence as a Legal Category: Doctrinal Approach to Formulating a Definition. – Actual Problems of Economics and Law 2020/1, lk 81. – https://heinonline.org/HOL/Page?public=true&handle=hein.journals/apel2020&div=8&start_page=79&collection=journals&set_as_cursor=0&men_tab=srchresults (24.02.2021).
[45] Russell, J.S. Norvig, P. Artificial Intelligence. A Modern Approach. Third Edition. New Jersey: Pearson 2010, lk 1.
[46] Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM/2018/237 final. Brussels, 25.04.2018. – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN (27.02.2021).
[47] Langemets, M. jt. Eesti keele seletav sõnaraamat. „Eesti kirjakeele seletussõnaraamatu” 2., täiendatud ja parandatud trükk. Tallinn: Eesti Keele Sihtasutus 2009. – https://www.eki.ee/dict/ekss/index.cgi?Q=tehisintellekt&F=M (27.02.2021).

arvutiteaduse instituudi koostatud õppevahend tehisintellektist defineerib tehisintellekti kui loomulikku intellekti jäljendamist, s.t arvutisüsteemi võime täita üldiselt inimmõistusega seostavaid ülesandeid.[48] Eelmainitud tehisintellekti mõiste definitsioonidest johtuvalt on ikkagi keskseks kohaks inimesekeskne lähenemine ehk samastatakse inimesele iseloomustavad funktsioonid konkreetsete eesmärkide saavutamiseks.

Kirjandusest leidub mitu kategooriat, kuhu tehisintellekt liigitatakse. Kitsas tehisintellekt (ingl *Narrow or Weak Artificial Intelligence*) kujutab endast algoritme, mis suudavad täita kõrge täpsusega konkreetset ülesannet suure hulga andmete olemasolul[49] (näiteks male mängimine, haiguste diagnoosimine).[50] Kitsas tehisintellekt suudab täita piiratud rida ülesandeid ning see on seotud katsetega arendada tehisintellekti täiustamaks inimintelligentsus, kuid mitte dubleerimaks seda.[51] Enamik kaasaegseid tehisintellekti süsteeme kuulub kitsa tehisintellekti kategooria alla.[52] Kitsa tehisintellekti tehnoloogial põhinevad rakendused on leidnud kasutuse tuntud firmades: Facebook-is piltide peal nägude identifitseerimine ja kasutajate märkimine, Siri käitumine vastavalt inimhääle mõistetud juhisele, isejuhtivate autode arendamine Tesla näitel.[53]

Üldine tehisintellekt (ingl *Artificial General Intelligence,* samuti tuntud ka *Strong Artificial Intelligence*) omab inimtasemel intelligentsust, mis hõlmab võimet mõtiskleda, kontekstist aru saada, kohaneda uute oludega ja täita keerukaid ülesandeid erinevates olukordades, mida kaasaegne kitsas tehisintellekt teha ei suuda.[54] Kuivõrd üldise tehisintellekti loomisega kaasnevad teatud tehnilised raskused, jääb veel ebaselgeks, millal üldise tehisintellekti alal

[48] Koit, M. Roosma, T. Tehisintellekt. Tartu Ülikooli arvutiteaduse instituut. Tartu: Tartu Ülikooli kirjastus 2011, lk 6. - https://dspace.ut.ee/bitstream/handle/10062/28296/tehisintellekt.pdf?sequence=2&isAllowed=y (27.02.2021).
[49] Tizhoosh, H.R. Pantanowitz, L. Artificial intelligence and digital pathology: Challenges and opportunities. – Journal of pathology informatic 2018/9, lk 2. – http://www.jpathinformatics.org/text.asp?2018/9/1/38/245402 (28.02.2021).
[50] Goertzel, B. Artificial general intelligence (Vol.2). Edited by Pennachin C. New York: Springer 2007, VI Preface.
[51] Haney, B. S. The perils and promises of artificial general intelligence. – Journal of Legislation 2018/45, No.2, lk 152-153. – https://heinonline.org/HOL/Page?handle=hein.journals/jleg45&div=10&g_sent=1&casa_token=&collection=journals (28.02.2021).
[52] Goertzel, VI Preface.
[53] Kaplan, A. Haenlein, M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. – Business Horizons 2019/62, No. 1, lk 16. – https://www.sciencedirect.com/science/article/pii/S0007681318301393 (28.02.2021).
[54] Ng, G.W. Leung, W.C. Strong Artificial Intelligence and Consciousness. – Journal of Artificial Intelligence and Consciousness 2020/7, No. 1, lk 64. – https://www.worldscientific.com/doi/epdf/10.1142/S2705078520300042 (08.03.2021).

toimuvad muudatused. Lähimas tulevikus ei oodata hetkel edusamme, pigem eeldatakse esimesi tulemusi näha kauges tulevikus.[55]

Kolmandasse tehisintellekti kategooriasse kuulub superintelligentsus (ingl *Artificial Superintelligence*). Kui üldist tehisintellekti ei ole veel olemas, siis superintelligentsus tundub rohkem ulmevaldkonnast pärinevat. Superintelligentsuse näol on tegemist tehisintellektiga, mille võimekus paljudes valdkondades on oluliselt suurem kui inimvõimed. Tulenevalt tema potentsiaalsest võimekusest võib välja töötatud superintelligentsus olla nii olulisel määral kasulik kui ka katastroofiliselt kahjulik olenevalt selle ülesehitusest. Superintelligentsuse kahjulikkuse tõenäosus oleneb eelkõige inimtegevusest, kuna inimestel on olemas võimalusi maandada sellega seonduvaid riske.[56]

Eelnimetatud tehisintellekti kategooriate kirjeldus on konspektiivne ning edasine käsitluse arendamine on väljaspool käesolevast magistritööst. Kokkuvõtvalt saab öelda, et hetkeseisuga on valitseva mõjuga kitsas tehisintellekt, mida kasutatakse erinevates eluvaldkondades, ning üldine ja superintelligentsus on tehisintellekti edasine areng, mille tulemustega saab inimkond tutvuda ilmselt kauges tulevikus, ning mille õiguslik reguleerimine sõltub juba nende kategooriate tehisintellekti olemusest, iseärasustest ja kaasnevatest riskidest.

Üldiselt on tehisintellekti lahutamatuks osaks algoritmidel põhinev masinõpe (ingl *machine learning*), mis kogub, töötleb ja kohaneb tegelikust maailmast pärinevate andmetega. Tehisintellekt ei ole võimeline edenema ilma püsiva ja katkematu andmevarustuseta laiendamaks oma teadmiste alust. Tagamaks tehisintellektile stabiilne areng, koguvad vastutavad töötlejad tohutus koguses isikuandmeid, seeläbi võimaldades algoritmidel nende andmete põhjal õppida.[57]

Masinõppe algoritme peetakse tehisintellekti aladistsipliiniks, mille omapära seisneb varasemate kogemuste kasutamises tulemuste parandamiseks või täpsete ennustuste

[55] Tizhoosh/Pantanowitz, lk 2.
[56] Baum, S. Barrett, A. Yampolskiy, R. Modelling and Interpreting Expert Disagreement About Artificial Superintelligence. – Informatica 2017/41, No. 7, lk 419-428. – https://ssrn.com/abstract=3104645 (08.03.2021).
[57] Humerick, M. Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence. – Santa Clara High Technology Law Journal 2018/34, No. 4, lk 395. – https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj34&div=19&id=&page= (09.03.2021).

tegemiseks,[58] tuvastades selleks kindlaid mustreid suurte andmete hulgas.[59] Võrreldes inimõppega, mille puhul mõõdetakse õppimisprotsessi tulemuslikkust funktsionaalses mõttes – kas inimene saab aja jooksul paremini hakkama konkreetse ülesandega enda kogemuse pinnalt, masinõppe süsteemid õppivad sarnaselt inimesega, st suudavad aja jooksul konkreetse ülesande täitmist parandada, uurides selleks rohkem andmeid ning otsides täiendavaid mustreid, mis aitavad omakorda paremini langetada automatiseeritud otsuseid.[60] Masinõppe täiuslikkus ja selle saavutamiseks kasutatavad tehnikad sõltuvad järgmistest peamistest teguritest: millist masinõppe komponent vajab täiustamist; milliseid eelnevaid teadmisi on süsteemil juba olemas; millisel kujul on andmed esitatud; millisest tagasisidest on võimalik õppida ehk kas andmete hulgas esineb mõnda anomaaliat, millest saab õppida.[61]

Tulenevalt masina õppimise tagasiside mehhanismi olemusest eksisteerib neli kõige levinumat õppimise tüüpi: juhendatud õpe (ingl *supervised learning*), juhendamata õpe (ingl *unsupervised learning*), pooljuhendatud õpe (ingl *semi-supervised learning*) ja stiimulõpe (ingl *reinforcement learning*).[62]

Juhendatud õppe puhul saab süsteem õppimiseks hulga välja valitud andmeid ning teeb ennustusi kõigi seni nägemata andmete osas.[63] Teiste sõnaga peab süsteem suutma uurida mõnda ette antud sisend-väljundpaari näidet, õppima tulemusest, mis viis sisendist väljundini,[64] teha üldistusi mõningatest näidetest ja ennustama neid variante, mis pole varasemalt talle õppimiseks antud näidetes demonstreeritud ning mis võivad tulevikus tekkida.[65] Juhendatud õppe näiteks on rämpsposti tuvastamine, mille puhul kvalifitseerib süsteem e-kirju rämpspostiks või tavaliseks kirjaks konkreetsete tunnuste, näiteks sõnade alusel.[66]

[58] Mohri, M. Rostamizadeh, A. Talwalkar A. Foundations of machine learning. Cambridge: The MIT Press 2018, lk 1.
[59] Surden, H. Artificial Intelligence and Law: An Overview. – Georgia State University Law Review 2019/35, lk 1131. – https://ssrn.com/abstract=3411869 (09.03.2021).
[60] *Ibidem*, lk 1311-1312.
[61] Russell/Norvig, lk 693-694.
[62] *Ibidem*.
[63] Mohri/Rostamizadeh/Talwalkar, lk 6.
[64] Russell/Norvig, lk 695.
[65] The European Commission`s High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines. Brussels, 08.04.2019, lk 3-4. – https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (11.03.2021).
[66] Mohri/Rostamizadeh/Talwalkar, lk 2-4.

Järgmine masinõppe tüübiks on juhendamata õpe, mille puhul saab süsteem õppimiseks sildistamata andmeid eesmärgil tuvastada andmetes teatud reeglipärasus ja rühmitada neid andmeid konkreetsesse rühma.[67] Pooljuhendatud õpe sisaldab nii juhendatud kui ka juhendamata õppe tunnuseid, nimelt kasutab nii sildistatud kui sildistamata andmeid konkreetse ülesande täitmiseks. Praktikas kasutatakse pooljuhendatud meetodit olukorras, kus ette antud andmete olemasolul pakuvad sildistamata andmed lisateavet, mis aitab andmete klassifitseerimise ennustamiseks saavutada parimat tulemust.[68]

Stiimulõppel peab süsteem teabe kogumiseks aktiivselt suhtlema ümbritseva keskkonnaga ning teatud juhtudel mõjutama seda keskkonda, mille tulemusena saab ta iga tegevuse eest kohest tagasisidet.[69] Seega süsteem õpib ja teeb otsuseid vastavalt kas positiivsele või negatiivsele signaalile[70] saamaks aru, kas ta teeb õige või vale otsuse, ning selle eesmärk on suurendada aja jooksul positiivseid signaale.[71] Stiimulõpet kasutatakse internetipõhistes soovitusüsteemides, mis soovitavad kasutajatele neile ostuhuvi pakkuvat kaupa.[72] On teine näide sellest õppest, kus kliendi jootraha puudus annab taksoteenust pakkuvale agendile märku, et ta tegi midagi valesti.[73]

Sügavõpe on masinõpe alamvaldkond, mis õpetab süsteemi töötlema sisendandmeid läbi nö kihtide hierarhiat, kus iga mõiste on määratletud lihtsamate mõistete suhtes, ning abstraktsemad esitused on arvutatud vähem abstraktsete esituste kujul, seeläbi võimalades süsteemil täiustada ennast kogemuste ja andmetega.[74] Sügavõppe algoritmid põhinevad neurovõrkude kontseptsioonil, millel on analoogselt inimneuronitele väikeste töötlemisüksuste võrk paljude kaalutud ühendustega.[75] Sellel neurovõrgul on mitu kihti sisendi ja väljundi vahel, mis aitab tõhusalt õppida kogu sisend-väljundi suhet, ning mis teeb sügavõppe tehnikat täpsemaks ja vähem inimese juhendamisest sõltuvaks.[76] Maailma tuntud ettevõtete *Google, Apple* ja *Facebook* projektid põhinevad sügavõppe tehnikal suure hulga andmete kogumiseks ja nende

[67] Mohri/Rostamizadeh/Talwalkar, lk 6.
[68] Van Engelen, J.E. Hoos, H.H. A survey on semi-supervised learning. – Machine Learning 2020/109, No.2, lk 1-2. – https://doi.org/10.1007/s10994-019-05855-6 (11.03.2021).
[69] Mohri/Rostamizadeh/Talwalkar, lk 7.
[70] Positiivse ja negatiivse signaalide asemel kasutatakse mõisted „tasustamine“ (ingl reward) ja „karistamine“ (ing *punishment*), vt Russell, J. S. Norvig P. Artificial Intelligence. A Modern Approach.
[71] European Commission. High-Level Expert Group on Artificial Intelligence, lk 4.
[72] *Ibidem.*
[73] Russell/Norvig, lk 695.
[74] Bengio Y, Goodfellow I, Courville A. Deep learning. Massachusetts: MIT press 2017, lk 5-8.
[75] European Commission. High-Level Expert Group on Artificial Intelligence, lk 4.
[76] *Ibidem.*

analüüsimiseks. Heade näidetena võib tuua Apple seadmel Iphone rakendatud Siri ehk seadme kasutajale erinevate teenuseid pakkuv virtuaalne isiklik assistent, mis võtab Apple poolt kogutud andmeid, või Google Translate ja Google Maps Street View lahendusega, kus kasutatud suureid andmeid (ingl *Big data*) saadetakse Internetist.[77]

Käesolevas magistritöös kasutatakse kitsa tehisintellekti mõistet, mis hõlmab hetkel teadaolevaid erinevaid masinõppe tehnikaid. Antud töös on kajastatud kõige levinumad masinõppe tehnikad, kuigi eksisteerivad ka muud tehisintellekti valdkonna seisukohalt olulised ja erinevates elusfäärides ja töölõikudes praktilist kasutust leitavad. Autor ei pea vajalikuks kirjeldama selles töös kõiki võimalikke masinõppe tehnikaid eelkõige nende paljususe tõttu ning teiseks, ei panda rõhku iga masinõppe tehnika spetsiifilistele omadustele, kuivõrd ei keskendu autor konkreetsetele rakendustele, kus tehisintellekti abil töödeldakse andmeid profiilanalüüsi koostamisel, vaid koondub tähelepanu selle protsessi läbipaistvusele ja sellega seonduvatele õiguslikele probleemidele.

1.3. Profiilanalüüsile tuginedes automatiseeritud otsuste vastuvõtmine tehisintellekti poolt

Isikuandmete kaitse üldmääruse artikli 4 punkt 4 defineerib profiilianalüüsi kui „igasugust isikuandmete automatiseeritud töötlemist, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamist, eelkõige selliste aspektide analüüsimiseks või prognoosimiseks, mis on seotud asjaomase füüsilise isiku töötulemuste, majandusliku olukorra, tervise, isiklike eelistuste, huvide, usaldusväärsuse, käitumise, asukoha või liikumisega.“ Sealjuures tuleb andmesubjekti teavitada profiilianalüüsi olemasolust ja selle analüüsi tagajärgedest.[78] Profiilianalüüs koosneb kolmest elemendist, esiteks peab protsess olema automatiseeritud, teiseks peab see toimuma isikuandmete töötlemisel, ja kolmandaks peab selle eesmärgiks olema füüsilise isiku isiklike aspektide hindamine.[79] Andmete

[77] Chen, X.W. Lin, X. Big Data Deep Learning: Challenges and Perspectives. – IEEE Access 2014/2, lk 514-515. – https://ieeexplore.ieee.org/abstract/document/6817512 (16.03.2021).
[78] IKÜM, põhjendus 60.
[79] The Article 29 Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251, lk 6-7. – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (20.04.2021).

töötlemisel kujutab profiilanalüüs ennast protsessi, mis hõlmab andmete kogumist, mille alusel teostatakse analüüs.[80]

Profiilianalüüsi saab laiendatult defineerida kui isikuandmete ja muude andmete koos töötlemist eesmärgiga luua teadmist teabe korrelatsioonide baasil, mida saab hiljem kasutada otsuste vastuvõtmise protsessis. Profiilianalüüs on seega korreleeritud teabe kogum, mis seostub kindla indiviidiga või indiviide grupiga.[81] Üldmääruse profiilanalüüsi definitsioon ei kirjelda töötlemise tegevust ennast, vaid selle töötlemise tulemit, hõlmates laia spektrit töötlemise situatsioonidest.[82] Profiilide konstrueerimine on protsess avastamaks teadmata mustreid suurte andmehulkade vahel, mida saab kasutada konkreetse profiili koostamisel. Taoliste profiilide rakendamine on indiviidi või indiviidide grupi seostamine konkreetse profiiliga ja selle baasil otsuse vastu võtmine. IKÜM toodud definitsioon seostab profiilianalüüsi ainult konkreetse indiviidiga, jättes kõrvale nö grupiprofiilid, millesse kuulumine võib samaväärselt indiviidi õiguseid ja vabadusi piirata.[83] Kui on kogutud piisavalt suur hulk teavet üksikute indiviidide eelistuste ja käitumise kohta, saab sellest luua grupiprofiili, mida saab kasutada inimeste edasiseks profileerimiseks. Kuulsaim näide sellest on skandaal, mis puhkes Cambridge Analytica taolisest profiilianalüüside koostamisel, mille eesmärk oli teha konkretiseeritud ennustusi ja samaaegselt ka võimalusel mõjutada tuhandete inimeste käitumist valimiste läbiviimisel.[84] Profiilianalüüsi koostamine võib kätkeda seega märkimisväärset riski mitte ainult indiviidile, vaid võib mõjutada laiemat inimgruppi, mille hulka konkreetne indiviid mingite näitajate tõttu kuulub.

Sellega seondub asjaolu, et isikuandmete kaitse üldmääruse üheks eesmärgiks on sammupidamine tehnoloogilise arenguga ja selle kaudu tulenevatest uutest ja teadmata riskidest. Infotehnoloogiline areng on andnud nii eraõiguslikele juriidilistele isikute kui ka avaliku võimu kandjatele võimalusele töödelda isikuandmeid järjest suuremal ja mõnedel juhtudel lausa hoomamata määral. Andmesubjektid avaldavad järjest enam enda isikuandmeid vabatahtlikult ja globaalsel skaalal.[85] Levinumateks vahenditeks taolise avaldamise jaoks on

[80] Rücker/Kugler, lk 265.
[81] Sartor, G. Lagioia, F. The impact of the General Data Protection Regulation (GDPR) on artifical intelligence. Brussels: European Parliamentary Research Service 2020. – https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (10.04.2021), lk 23.
[82] Voigt/Von dem Bussche, lk 181.
[83] Sartor/Lagioia, lk 23.
[84] *Ibidem*, lk 23-24.
[85] *Ibidem*.

erinevad sotsiaalmeedia platvormid. Isikuandmete avaldamine on muutunud sotsiaalse elu osaks.

Automatiseeritud otsuseid võidakse vastu võtta kas koos profiilianalüüsiga või ilma, kuid need kaks elementi ei pea olema tingimata eraldatud. Profiilianalüüsi saab eelkõige kasutada üldiselt, otsuste vastuvõtmisel ja otsuste vastuvõtmisel üksnes automatiseeritud viisil, millest tulenevad õiguslikud või muud märkimisväärsed mõjud andmesubjektile. Teisel näitel võetakse otsus vastu inimese poolt, kes kasutab selleks automaatselt koostatud profiilianalüüsi. Kolmandal juhul võetakse otsus vastu automaatselt algoritmile tuginedes ja otsus on kehtiv ilma inimsekkumiseta. [86] Vastutavad töötlejad võivad teostada profiilianalüüsi või automatiseeritud otsuste vastuvõtmist ainult juhul, kui on töötlemine on kooskõlas isikuandmete kaitse põhimõtetega ja teevad seda seaduslikul alusel.[87]

Lähtuvalt IKÜM artikli 6 lõike 1 punktidest a-f on välja toodud ammendav isikuandmete töötlemise seaduslike aluste loetelu, milleks on andmesubjekti nõusolek, lepingu täitmine või lepingu sõlmimine, juriidiline kohustuse täitmine, isiku eluliste huvide kaitsmine, ülesande täitmine avalikes huvides või avaliku võimu teostamine, vastutava töötleja või kolmanda isiku õigustatud huvi korral, mis kaalub üles andmesubjekti huvid, põhiõigused ja -vabadused. Kõige enam huvipakkuvam käesoleva töö vaatest on alternatiiv, mil otsused võetakse vastu ilma inimsekkumiseta.

Profiilianalüüsi koostamist ja automatiseeritud otsuste vastuvõtmist kasutatakse paljudes erinevates majandusharudes, olgu selleks nii avalik või erasektor. Otsustusprotsesside tõhustamiseks kasutatakse profiilianalüüsi aina enam just panganduses, tervishoius, kindlustuse pakkumises, turunduses ja paljudes muudes valdkondades.[88] Eelkõige peaks taoline protsess suurendama efektiivsust ja aitama kaasa ressursside kokkuhoiule.[89] Näiteks tulenevalt Swedbank Eesti kliendiandmete töötlemise põhimõtetest, kasutatakse „profiilianalüüsi kliendi nõustamisel, turunduse eesmärgil ja automatiseeritud otsuste tegemisel näiteks laenuvõime hindamiseks, riskijuhtimiseks, kindlustusriskide hindamiseks ning tehingute kontrollimiseks pettustega võitlemisel. Samuti kasutab Swedbank profiilianalüüsi ja automatiseeritud otsuste

[86] The Article 29 Working Party, WP251, lk 8-9.
[87] IKÜM, põhjendus 72.
[88] The Article 29 Working Party, WP251, lk 5.
[89] *Ibidem*, lk 5.

tegemist, et parandada teenuste kasutamise kogemust, mille hulka võib kuuluda eesmärk kohandada teenuste kuvamist kasutatavatele seadmele ja luua klientidele sobivaid pakkumisi.“[90] Isikuandmete hulk, mida pangad töötlevad, ja nendest järelduste tegemise võimalikkus on suuremahuline. Kliendi kaardimaksete andmetele tuginedes võib järeldada lugematuid seoseid isiku eraelu kohta, sealhulgas tema töökohta, tööaega, teiste isikute kokkupuuteid isikuga, ühiskondlikku kuuluvust, sugulussidemeid, liikumist reaalajas ja palju muud.

Rahapesu ja terrorismi rahastamise tõkestamise seaduse (edaspidi RahaPTS)[91] § 48 lõike 2 alusel on krediidiasutusel kui kohustatud isikul on lubatud kogutud isikuandmeid töödelda üksnes rahapesu ja terrorismi rahastamise tõkestamise eesmärgil (nt seadusest tulenevate hoolsusmeetmete täitmiseks) ning neid andmeid ei tohi täiendavalt töödelda viisil, mis ei vasta nimetatud eesmärgile, näiteks turunduslikel eesmärkidel. Automatiseeritud protsessi käigus võib kogutud isiku kaardimaksete ja sularaha sissemaksete andmete põhjal tuvastada rahapesu kahtlusele või terrorismi rahastamisele viidatud asjaolud, näiteks kontole laekunud suuremahulisest rahasummast osade kaupa sularaha väljavõtmine erinevates välisriikides asuvate erinevate sularahaautomaatide kaudu. Antud profiilanalüüsi näitel kaardistab ja tuvastab automatiseeritud protsessi riskid, kuid lasta süsteemil automaatselt hinnata neid tulemusi ja teha otsustusi rahapesu või terrorismi rahastamise kontekstis on ikkagi suur kaalutluskoht.

Analüüsides eeltoodud näidet, kitsa tehisintellekti süsteemil puudub inimintelligentsust subsumeerida sellist tehingute mustrit taustal olevate eluliste asjaoludega, milleks võib olla kõrgepalgalise isiku tööülesannete täitmise ja iseloomuga seotud vajadus käia tihti lähetustel välisriikidesse, kus on mugavam kasutada arveldamiseks sularaha. Inimene suudab mõistlikult tausta ja tehingute asjaolusid arvesse võtta ning selle põhjal hinnata, kas kaardi- ja sularahamaksed annavad käesoleval juhul piisava aluse kahtlustada rahapesu või terrorismi rahastamist.

[90] Swedbank AS Kliendiandmete töötlemise põhimõtted, lk 3. – https://www.swedbank.ee/static/pdf/private/home/important/gdpr/Principles_of_processing_Personal_data_EE_EST_01032021.pdf (01.03.2021).
[91] Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 17.11.2017, 2.

Andmesubjektil peaks olema üldjuhul õigus sellele, et „tema suhtes ei tehta üksnes andmete automatiseeritud töötlemisele toetuvat isiklikke aspektide hindamisel põhinevat ja meedet sisaldada võivat otsust, millel on teda puudutavad õiguslikud tagajärjed või mis avaldab talle samamoodi märkimisväärset mõju“ ilma inimsekkumiseta.[92] Taolised õiguslikud tagajärjed peavad mõjutama indiviidi põhiõigusi, nt vabadust teistega suhelda, valimistel osaleda. Õiguslik tagajärgi võib olla seotud ka asjaoludega, mis mõjutavad indiviidi õiguslikku staatust või tema õigusi lepingulistes suhetes. Automatiseeritud otsuste õiguslikuks tagajärjeks võivad seega olla näiteks teatava lepingu lõpetamine, riigi või kohaliku omavalitsuse poolt antavate toetuste ja hüvitiste saamine või nende maksmisest keeldumine, riiki sisenemise õigusest või kodakondsuse andmisest keeldumine.[93] Kui otsusel isiku põhiõigustele ei ole, võivad regulatsiooni alla langeda ka muud otsused, mis omavad isikule märkimisväärset mõju. Isikuandmete automatiseeritud töötlemise põhjal vastu võetud otsus võib isikule märkimisväärset mõju avalda eelkõige juhtudel kui need märkimisväärselt mõjutavad isiku elutingimusi, käitumist või otsuseid, kui need omavad isikule pikaajalist või permanentset mõju, või need viivad isiku diskrimineerimise võimaluseni. Otsused, mis võivad taolist mõju avaldada on eelkõige otsused, mis mõjutavad isiku majanduslikku heaolu, nt mõju tema laenuvõimele, otsused, mis mõjutavad isiku juurdepääsu tervishoiuteenustele, otsused, mis takistavad isikul töösuhtesse astuda või panevad teda ebasoodsasse positsiooni, või otsused, mis mõjutavad isiku juurdepääsu haridusele, nt ülikooli sisseastumise taotlus.[94]

Regulatsiooni mõju alt jäävad seega välja otsused, mis eelpool mainitud mõju isikule ei avalda. Selle puhul tuleb arvestada, et otsused, mis ei oma tavapäraselt märkimisväärset mõju, võivad taolist mõju avaldada konkreetsesse sotsiaalsesse gruppi kuuluvatele isikutele, mis eeldaks otsuste tegemisel erinevate tingimuste arvestamist.

Taoline „profiilianalüüsil põhinev otsuste tegemine peaks olema samas lubatud siis, kui see on sõnaselgelt lubatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega, muuhulgas pettuste ja maksudest kõrvalehoidumise järelevalve ja ennetamise eesmärkidel. Lisaks peaks olema see taoline töötlemine lubatud, kui see on vajalik andmesubjekti ja

[92] IKÜM, põhjendus 71.
[93] The Article 29 Working Party, WP251, lk 21.
[94] *Ibidem,* lk 21-22.

vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks või siis, kui andmesubjekt on andnud selleks selgesõnalise nõusoleku.“[95]

Eelpool toodust lähtuvalt sisaldab IKÜM artikkel 22 endas üldist keeldu võtta vastu otsuseid andmesubjekti kohta, mis põhinevad üksnes automatiseeritud töötlemisel, sealhulgas profiilianalüüsil, mis toovad kaasa andmesubjekti puudutavaid õiguslikke tagajärgi või avaldavad talle märkimisväärset mõju. Üldmääruse artikkel 22 viitab otsustele, mis on tehtud ainult automatiseeritud protsessidele tuginedes, seega puudub inimsekkumine täielikult. Üldisele keelule on erandid, mille osade rakendumisel tuleb teatavate meetmetega tagada andmesubjekti õigused, vabadused ja õigustatud huvi.[96]

Tulenevalt IKÜM artikli 22 lõikest 2 on erandiks otsus, mis „on vajalik andmesubjekti ja vastutava töötleja vahelise lepingu sõlmimiseks või täitmiseks, mis on lubatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega“, ja mis põhineb andmesubjekti selgesõnalisel nõusolekul.

Vastutavatel töötlejatel on olemas suur tahe kasutada automatiseeritud otsuste vastuvõtmist lepingu sõlmimiseks või selle täitmiseks. Regulaarne inimsekkumine oleks paljudel juhtudel ebapraktiline või lausa võimatu, tulenedes töödeldavate andmete suurest hulgast. Sellegipoolest peab vastutav töötleja olema suuteline näitama, kas selline töötlemine on vajalik. Kui otsuste vastuvõtmiseks on võimalik kasutada muid vähem õigustele mõju avaldavat võimalust, ei saa automatiseeritud otsustusprotsessi pidada vajalikuks. Automatiseeritud otsuste vastuvõtmine on lubatud ka juhul, kui taoline õigus on sedastatud vastutava töötleja suhtes kohaldatava liidu või liikmesriigi õigusega, mis peab sellise õiguse andmisel endas sisaldama meetmeid, mis kaitsevad andmesubjekti õigusi ja vabadusi. Viimane erand eeldab andmesubjekti selgesõnaline nõusolekut, mis tuleneb asjaolust, et automatiseeritud otsuste tegemine kätkeb endast märkimisväärset isikuandmete kaitse riski. [97]

Üldmääruse artiklis 22 puudub otsene keeld kasutada automatiseeritud otsuste vastuvõtmist otsuste puhul, mis on seotud lastega, kuid vastutavatel töötlejatel pole soovituslik tugineda

[95] IKÜM, põhjendus 71.
[96] The Article 29 Working Party, WP251, lk 19.
[97] *Ibidem,* lk 23-24.

artiklis toodud eranditele. Tavapäraselt märkimisväärset mõju mitte avaldavad otsused võivad taolist mõju avalda lastele. Eriti tuleb seda arvestada lastele suunatud reklaami pakkumisel kasutades selleks profiilianalüüsi. Igasugused kaitsemeetmed, mis on artiklis 22 toodud, peavad olema sellisel juhul asjakohased lapsi arvestades ja vastutav töötleja peab tagama, et need meetmed on efektiivsed.[98]

Andmesubjekti õiguste, vabaduste ja õigustatud huvi kaitseks kehtivad meetmed peavad sisaldama vähemalt õigust otsesele isiklikule kontaktile vastutava töötlejaga, õigust väljendada enda seisukohta töötlemise kohta ning õigust otsust vaidlustada.[99] Otsuse vastuvõtmist üksnes profiilianalüüsile tuginedes ilma inimsekkumiseta tuleb tõlgendada kitsalt, st inimsekkumine peab olema sisuline ja teostatud indiviidi poolt, kel on volitus ja pädevus otsust muuta. Vastutava töötleja poolt kogutud teave isikuandmete töötlemise kohta peab sealjuures näitama, millisel määral ja staadiumis vastav inimsekkumine toimub.[100] Üksnes profiilianalüüsile tuginedes otsuse vastuvõtmine on lubatud juhul, kui see on vajalik lepingu sõlmimiseks või selle täitmiseks andmesubjekti ja vastutava töötleja vahel. Sellist vajalikkust tuleb sisustada samuti kitsalt, kui eesmärki on võimalik mõistlikult ja efektiivselt saavutada muudel vähem andmesubjekti õigusi piiraval viisil, pole taoliste otsuste vastuvõtmine enam vajalik.[101]

Tehisintellekti rakendamisel otsuste vastuvõtmisel tähendab eelduslikult, et enamik neist otsuseid on vastu võetud ilma inimsekkumiseta. Järjest enam saab rääkida juhtudest, kus sisuline inimesekkumine võib olla võimatu, tulenedes puudulikule ligipääsule andmetele, mida tehisintellekt suudab kasutada ja kasutab, ning asjaolule, et inimene ei suuda enam efektiivselt tehisintellekti otsustusprotsessi analüüsida. See võib tekitada olukorra, kus otsuste vastuvõtmise eest võib inimene küll vastutada, kuid see vastutus on formaalset laadi, täitmata järelevalve eesmärke.[102]

Tehisintellekti poolt profiilianalüüsil põhinevate otsuste vastuvõtmisel peab eelkõige olema tagatud otsuse läbipaistvus, mis võib tulenedes tehisintellekti olemusest olla märkimisväärselt

[98] The Article 29 Working Party, WP251, lk 28-29.
[99] Sartor/Lagioia, lk 62-63.
[100] The Article 29 Working Party, WP251, lk 21.
[101] Buttarelli, G. Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: a Toolkit. Brussels: European Data Protection Supervisor 2017, lk 8. – https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf (03.04.2021).
[102] Sartor/Lagioia, lk 60.

keeruline. IKÜM artikli 13 lõike 2 punkti f on vastutaval töötlejal kohustus teavitada andmesubjekti, et taolisi otsuseid võetakse vastu, anda andmesubjektile sisulist teavet otsuste vastuvõtmise loogika kohta, ning anda teavet selle kohta, millised on sellise isikuandmete töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks. Olenevalt faktilisest olukorrast ja otsuse raskusastmest võib taoline teave olla väga laiapõhjaline. Eeltoodud teabe hulka kuulub üldine informatsioon vajalike sisendite ja väljundite osas ja mis tähtsus omavad erinevad sisendid otsuse vastuvõtmisel. Täpne teave, mida on kogutud indiviidi kohta, ja mida on kasutatud profiilianalüüsi koostamisel.[103] Sisulise teabe andmine on aina enam keerulisem tulenevalt masinõppe protsesside kiirest arengust, kuid vastutav töötleja peab andma endast parima, et seda andmesubjektile lihtsal viisil selgitada, miks ja millisel alusel taolised otsused vastu võetakse.[104]

Kokkuvõtlikult on tehisintellekti rakendamine profiilianalüüsi koostamisel ja selle põhjal üksikotsuste vastuvõtmisel on mitmes majandusvaldkonnas igati loogiline samm, kuid selle juures tuleb sellegipoolest täita isikuandmete kaitse nõudeid. Tulenevalt tehisintellekti olemusest ja järjepidevast arengust on taoliste nõuete täitmine vastutavate töötlejate poole aina keerulisem, johtudes eelkõige otsuste kontrollimise vajadusest ja selle võimalikkusest.

Andmesubjekti teavitamine tehisintellekti poolt profiilanalüüsil põhinevate otsuste langetamise protsessi kirjeldusest tekitab olukorra, kus vastutav töötleja võib olla sunnitud avaldama enda ärisaladust või krediidiasutuse näitel lisaks ka pangasaladust, jagades oma organisatsiooni sisemisi protseduurireegleid ja isiku kohta koostatud hinnanguid, milles võivad sisaldada teiste isikute andmeid. Üldjuhul inimsekkumine tehisintellekti poolt isikuandmete töötlemise protsessi aitab ära hoida tehisintellektile töötlemiseks antud andmete pinnal väärtõlgendusi andmesubjekti kahjuks ja taolise töötlemisega kaasnevaid organisatsioonile avalduvaid negatiivseid mõjusid.

[103] Sartor/Lagioia, lk 64-65.
[104] The Article 29 Working Party, WP251, lk 25.

1.4. Üldised nõuded tehisintellekti läbipaistvusele ning selle võrdväärsus IKÜM-i läbipaistvuse põhimõttele

Käesolevas alapeatükis keskendutakse tehisintellekti läbipaistvuse kontseptsioonile aru saamaks, mis peetakse selle käsituse all ja millistele nõuetele peab tehisintellekti vastama selle läbipaistvuse saavutamiseks. Täiendavalt peab analüüsi käigus andma vastust magistritöö sissejuhatavas osas seatud uurimisküsimusele, mis puudutab võimalust õiguslikult maandada tehisintellekti süsteemi rakendamisega kaasnevaid riske profiilanalüüsi koostamisel ja tagada andmesubjektide põhiõiguste kaitse.

Üldiselt tähendab läbipaistvus organisatsiooni või selle osaleja kohta teabe kättesaadavust, mis võimaldab süsteemivälistel osalistel jälgida organisatsiooni sisemist töökorraldust ja tulemuslikkust.[105] Täpsemalt tehisintellekti kontekstis mõistetakse aga läbipaistvuse all analüüsitavate andmete ja masinõppe mudelite aluseks olevate mehhanismide avatust ja kommunikatsiooni.[106] Järelikult tehisintellekti läbipaistvuse käsitlus taandub sellele, kuidas saab mõõta, selgitada ja põhjendada andmete ja algoritmide sünergiat tehisintellekti süsteemides vältimaks seeläbi andmesubjekti suhtes võimalikke negatiivseid tagajärgi.

Mõistmaks tehisintellekti läbipaistvuse tagamise vajadust, tuleb esmalt määratleda, miks selle saavutamine on tänapäeval oluline otsustus õigusraamistikus. Tehisintellekti läbipaistmatus komplitseerib potentsiaalsete õigusrikkumiste tuvastamist ja tõendamist, vastutuse omistamist, kahjunõuete esitamise tingimuste täitmist ja õigusemõistmisele juurdepääsu tulemuslikkust negatiivse mõjuga otsuste puhul, mistõttu võib tekkida olukord, kus asjakohaste vahendite puudulikkuse tõttu ei ole võimalik kontrollida, kuidas jõuti konkreetse otsuseni selle tegemisse tehisintellekti kaasamisel ning kas asjaomastest normidest peeti kinni või mitte.[107]

[105] Robinson, S. C. Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). – Technology in Society 2020/63, lk 3. – https://doi.org/10.1016/j.techsoc.2020.101421 (05.04.2021). Vt ka Grimmelikhuijsen, S. Porumbescu, G. Hong, B. Im, T. The effect of transparency on trust in government: A cross-national comparative experiment. – Public Administration review 2013/73, No. 4, lk 575-586. – https://doi.org/10.1111/puar.12047 (05.04.2021).
[106] Lepri, B. Oliver, N. Letouzé, E. Pentland, A. Vinck, P. Fair, Transparent, and Accountable Algorithmic Decision-making Processes. – Philosophy & Technology 2018/31, No. 4, lk 615. – https://link.springer.com/article/10.1007/s13347-017-0279-x#citeas (04.04.2021).
[107] Euroopa Komisjon. Valge raamat tehisintellekti kohta, lk 14-15.

Kuivõrd järjest kasvav keerukate tehisintellekti süsteemide kasutamine muudab võimalikke diskrimineerimise juhtumeid vähem jälgitavaks, lisab tehisintellekti läbipaistvuse saavutamine rohkem õiglust otsustusprotsessi tulemuste juurde.[108] Tulenevalt iseõppivate algoritmide ja tehisintellekti süsteemide keerukusest ei ole võimalik täielikult masinõppe käigus välja töötatavaid mudeleid ette näha, suunata ega seletada,[109]mistõttu tehisintellekti läbipaistvate süsteemide arendamine võimaldab selgitada, kuidas sai konkreetne otsus tehtud ja milliste andmete alusel.

Mõistagi võivad olla tehisintellektil põhinevad süsteemid ühe sidusrühma esindajatele arusaadavad, kuid teisele mitte. Sellest tulenevalt peab arvestama mitme osapoole tausta, teadmiste ja vajadustega jõudmaks ühtse läbipaistvuse eesmärgini, et:[110]

- Arendaja (ingl *Developer*), kes loovad otsustussüsteeme, saaks aru, kuidas tema poolt loodud süsteem töötab ja mis töötab õigesti või valesti, oskama seletada süsteemis toimuvaid kõrvalekaldeid, püüdes neid siluda või süsteemi parandada.[111] Diskrimineerivate tulemusteni viivate algoritmide põhjused peiduvad tavaliselt algoritmi kasutatavates andmetes, algoritmi modelleerimises ja selles, kuidas algoritmi kasutatakse.[112]
- Rakendaja (ingl *Deployer*), kes juurutab süsteemi oma majandustegevuses ja toob selle süsteemi kasutajate ette, tagaks kasutajale usaldustunnet, et viimane kasutaks jätkuvalt süsteemi.[113]
- Regulaator, sh õiguseksperdid, kes peavad vastanduma nendele süsteemidele, kasutades eetilist ja õiguslikku raamistikku, mõistaks mitte ainult, kui süsteemi välja antud täpne ennustus on, vaid ka seda, et kas langetatud otsus oli õigustatud, milliste õigusnormidega arvestati sealjuures, kas saab seada kahtluse alla süsteemi õiglast

[108] Van Nuenen, T. Ferrer, T. X. Such, J. M. Cote, M. Transparency for Whom? Assessing Discriminatory Artificial Intelligence. – Computer 2020/53, No. 11, lk 37. – https://ieeexplore.ieee.org/abstract/document/9237325 (27.04.2021).
[109] Pilving, I. Mikiver, M. Kratt haldusorganiks: algoritmilised otsused ja haldusõiguse põhimõtted. – Kohtute aastaraamat 2019. Tartu: Riigikohus 2019. – https://aastaraamat.riigikohus.ee/kratt-haldusorganiks-algoritmilised-otsused-ja-haldusoiguse-pohimotted/#_ftn33 (05.04.2021).
[110] Weller, A. Transparency: motivations and challenges. In Explainable AI: Interpreting, Explaining and Visualizing Deep Learning. Cham: Springer 2019, lk 23-40. – https://link.springer.com/chapter/10.1007/978-3-030-28954-6_2 (27.04.2021).
[111] *Ibidem.*
[112] Van Nuenen (jt), lk 38.
[113] Weller, 2-3.

toimimist ka teiste otsuste suhtes, milliseid isikuomadusi kasutati tulemuse ennustamiseks.[114] Eesmärgiks on ka võimaldada regulaatoril teostada järelevalvet süsteemi alusel tuletatud ennustuste või otsuste üle eriti nendeks puhkudeks, kui ennustus või otsus toob negatiivseid tagajärgi süsteemi kasutajale.[115]

- Kasutaja, keda mõjutavad loodud süsteemid, mõistaks, mida süsteem teeb ja miks, kuidas jõuti konkreetse otsuseni, kuna see võimaldab ennustada, mida süsteem võib ettenägematutes olukordades teha ja kontrollida süsteemi nõuetekohast toimimist, ning laiemalt loob usaldust tehnoloogia vastu, ületades hirmu teadmatuse ees.[116]

Järelikult aitab tehisintellekti läbipaistvuse tagamine aitab kujundada sellest ühetaolist arusaama igas eluvaldkonnas, kus saab rakendada tehisintellekti tehnoloogiat. Teiseks, igaühel peaks tekkima usaldus kasutatava süsteemi vastu vältimaks arusaamatusi ennustuste või langetatud otsuste osas, vaidlusi erinevate osapoolte vahel ja võimalikke ebasoodsaid mõju süsteemi kasutajale, kelle õigusi võib osutuda keeruliseks kaitsta tulenevalt selle konkreetse süsteemi ekspluateerimisest tingitud kahju või mõju olulisusest. See eeldab ka kõigi osapoolte omavahelist koostööd, kuivõrd tehisintellekti läbipaistvuse kontseptsiooni sisustab ja kujundab enda pädevuse piires iga osapool erinevalt lähtudes enda professionaalsetest kogemustest ja teadmistest. Kõike eespool kirjeldatut arvesse võttes, saab nentida selgitatavuse vajadust tehisintellektist tulenevate süsteemide ja kasutatavate algoritmide, nende arendamise ja rakendamise, ning õiguslike reguleerimise, kontrolli ja järelevalve järele.

Tehisintellekti läbipaistvus seostub tihedalt selgitatavuse (ingl *explainability*) põhimõttega, mis hõlmab andmete, ärimudelite ja protsesside läbipaistvust, süsteemide suutlikkusest ja otstarbest avalikku teavitamist ning otsuste arusaadavust ja jälgitavust eriti selliste puhkudeks, kus see avaldab inimelule märkimisväärset mõju, et oleks võimalik nõuda kohast, õigeaegset ja kohandatud asjaomase sidusrühma kvalifikatsiooniga selgitust nii tehisintellekti süsteemi otsuse tegemise protsessi kui ka organisatsiooni otsustusprotsessi kohta ning nõuetekohaselt neid otsuseid vaidlustada.[117]Algoritmi kasutaja ei pruugi alati eristada, milliseid muutujate vahelisi seoseid arvestatakse algoritmi klassifikatsiooni või millises algoritmi staadiumis see

[114] Van Nuenen (jt), lk 39.
[115] Weller, lk 3.
[116] *Ibidem.*
[117] The European Commission's High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. Brussels, 08.04.2019, lk 14, 18, 20. – https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (05.04.2021).

toimub, ega kindlaks määrata, kuidas täpselt algoritm koostab erinevaid seoseid muutujate vahel saavutamaks lõpptulemuse, mistõttu kirjeldatud algoritmide nähtust nimetatakse tehisintellekti läbipaistmatuseks (ingl *opacity* või *the lack of transparency*) ehk musta kasti (ingl *black box*) algoritmideks.[118]

Selgitatavuse vajaduse määr sõltub suuresti iga konkreetse juhtumi taustast ja puuduliku või hoopis ebatäpse otsuse tagajärgede tõsidusest, mistõttu võib osutuda tarvilikuks kasutusele võtta ka muud selgitatavuse meetmed süsteemi võimaluste kohta:

- jälgitavus (ingl *traceability*), et nii tehisintellekti süsteemi otsuse aluseks olevad andmekogumid ja protsessid kui ka tehisintellekti süsteemi tehtud otsused oleksid nõuetekohaselt dokumenteeritud tuvastamaks tehisintellekti väära otsuse põhjusi ja seeläbi vältimaks tulevikus vigu;
- auditeeritavus (ingl *auditability*), et võimaldada algoritmide, andmete ja projekteerimisprotsesse hinnata;
- teabevahetus (ingl *communication*), et informeerida inimesi kommunikeerimisel tehisintellekti süsteemiga, mh süsteemi suutlikkusest ja piirangutest konkreetsel asjakohasel juhul ning pakkuda võimalust suhelda selle asemel inimesega tagamaks põhiõiguste järgmist.[119]

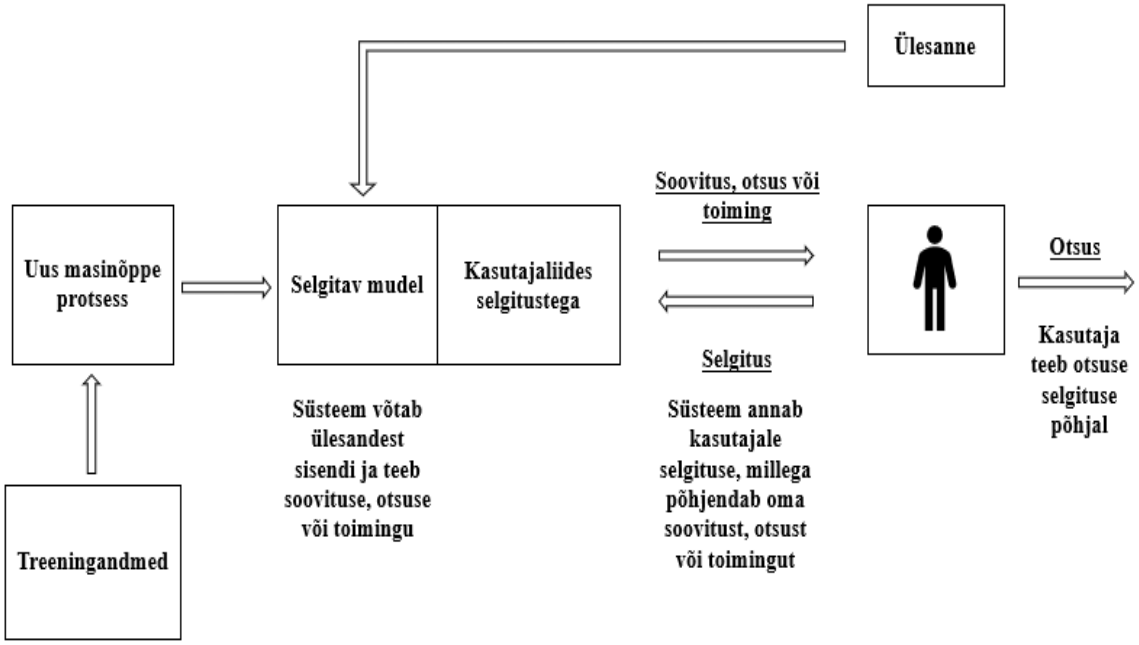
Tehisintellekti läbipaistmatuse probleemi lahendamisel hakati samuti arendama selgitavat tehisintellekti (ingl *Explainable Articicial Intelligence*, lüh xAI) selleks, et selgitada või aidata inimestel tõlgendada, kuidas konkreetne masinõppemudel oma järelduseni jõudis.[120] Näiteks 2017.aastal käivitas Ameerika Ühendriikide kaitseministeeriumi teadus- ja arendusagentuud *Defense Advanced Research Projects Agency* (edaspidi *DARPA*) selgitava tehisintellekti projekti,[121] mille eesmärgiks luua uusi või muuta olemasolevaid masinõppe tehnikaid sellisel viisil, et need toodaks n-ö selgitavaid mudeleid võimaldamaks lõppkasutajal mõista

[118] Coglianese, C. Lehr, D. Regulating by Robot: Administrative Decision Making in the Machine-Learning Era. – The Georgetown Law Journal 2017/105, No. 5, lk 1159. – https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2736&context=faculty_scholarship (07.04.2021).
[119] The European Commission's High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI, lk 20.
[120] Deeks, A. The judicial demand for explainable artificial intelligence. – Columbia Law Review 2019/119, No. 7, lk 1833-1834. – https://www.jstor.org/stable/26810851 (19.04.2021).
[121] Gunning, D. Aha, D. DARPA's Explainable Artificial Intelligence (XAI) Program. – AI Magazine 2019/40, No.2, lk 44-58. – https://doi.org/10.1609/aimag.v40i2.2850 (14.04.2021).

tehisintellekti süsteemide toimimise loogikat ja nende võimalikku tulevast käitumismustrit ja tõhusalt hallata tehisintellekti süsteeme.[122]

DARPA selgitava tehisintellekti kontseptsiooni kohaselt töötab tehisintellekti süsteem välja hulga uusi või muudetud masinõppetehnikaid tootmaks selgitavamaid mudeleid, seejärel integreeritakse inimese ja arvuti vahelised suhtlemistehnikad uute põhimõtete, strateegiate ja tehnikatega selgituste loomiseks ning selle tulemusena teeb süsteem järeldusi.[123] DARPA selgitava tehisintellekti kontseptsioon on alljärgnevalt näitlikustatud.

Tabel 1. Selgitavuse raamistik



Allikas: DARPA. Broad Agency Announcement on Explainable Artificial Intelligence (XAI), lk 6,13.

On olemas ka muid selgitava tehisintellekti meetodeid, millega modelleeritakse lihtsama ning arusaadavama algoritmiga keerulise rakenduse tööd või konstrueeritakse küll analoogne aga näilik olukord jättes korraga osa muutujaid kõrvale või neist mõnd muutes ja teise osa muutujaid muutumatuks, mille korral jõuab algoritm teise järelduseni.[124] Kuigi mitmeid selgitava tehisintellekti süsteeme on juba olemas ja uute süsteemide tehnikaid on loomas,[125] ei

[122] The Defence Agency Research Projects Agency. Broad Agency Announcement on Explainable Artificial Intelligence (XAI). Arlington, 10.08.2016. – https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf (19.04.2021).
[123] *Ibidem*, lk 6-7.
[124] Pilving/Mikiver, punkt 3.7.
[125] Deeks, lk 1834.

ole autorile teadaolevalt selliseid süsteeme laialt rakendatud või kasutusele võetud. Viimasest tulenevalt võivad selgitava tehisintellekti süsteemi rakendamisega kaasneda üpriski suured kulutused integreerimaks neid enda majandustegevusesse. Üldjuhul peab sarnaselt tehisintellekti süsteemidele õiguslikult reguleerida ka selgitava tehisintellekti süsteeme, välja kujundades õiguslikku raamistikku, mis kindlustab süsteemide protsesside ja otsuste usaldusväärsus ja läbipaistvus.

Eetikasuunistes usaldusväärse tehisintellekti arendamiseks rajaneb usaldusväärse tehisintellekti saavutamise raamistik nii Euroopa Liidu põhiõiguste hartas, Euroopa Liidu aluslepingutes ja rahvusvahelises inimõigustealases õiguses sätestatud põhiõigustel. Usaldusväärse tehisintellekti kontseptsioon hõlmab tehisintellekti seaduslikkust, eetilisust ja töökindlust. Põhiõiguste järgimine kuulub nii tehisintellekti seaduslikkuse kui ka selle eetilisuse aspektide alla, kuivõrd põhiõigustes peegelduvad kõigi isikute omapärased isiklikud ehk moraalsed õigused sõltumata nende õiguslikust siduvusest.[126]

Tehisintellekti läbipaistvuse nõue on üks olulisi eetikapõhimõtetel tuginevaid nõudeid, mida tuleb täita kogu tehisintellekti elutsükli jooksul. Seega peaksid üldjuhul tehisintellekti süsteemide arendamisse, rakendamisse ja õiguslikku reguleerimisse kaasatud osapooled suutma tagada tehisintellekti läbipaistvuse nõude kohaldamist ja täitmist, et süsteemi kasutajal oleks piisavalt informeeritud rakendatavatest süsteemidest ja oleks tal võimalik ühtlasi nõuda ka nii tehisintellekti läbipaistvuse nõude kui ka teiste tehisintellektile seatud nõuete järgimist.[127] Küsimus taandub aga praktilisele poolele, kas tehisintellekti läbipaistvusega seostuvad selgitatavuse, jälgitavuse, auditeeritavuse ja teabevahetuse meetmed võimaldavad sidusrühmadel piisaval määral saavutada tehisintellekti läbipaistvust, mida käsitleb käesolev töö järgnevalt.

Tegelikkuses, kus tehisintellekti algoritmid õpetavad ennast ise varasemate kogemuste pinnalt ning tuvastavad kindlaid mustreid kasutades selleks hulk andmeid konkreetse ülesande lahendamiseks, võib selgitatavuse tagamine osutuda problemaatiliseks. Autori hinnangul ei ole võimalik tõhusalt täita tehisintellekti poolt otsustustprotsesside selgitatavust ilma muude täiendavate meetmeteta, s.o auditeeritavus, jälgitavus ja teabevahetus, toetudes töös varasemalt

[126] High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI, lk 6-7.
[127] *Ibidem,* lk 8, 14.

avaldatule, et tänapäeval ei ole tehisintellekti valdkonna ekspert alati suuteline alati seletama, kuidas algoritmid jõudsid kindlale järeldusele. Ainult ühest eespool kirjeldatud meetmest ei piisa täielikult saavutamaks tehisintellekti läbipaistvust, pigem peab neid meetmeid kogumis hinnata ja tõhusalt rakendama läbipaistvuse tagamise eesmärgil. Seega on selgitatavuse rakendamine tulevikuperspektiivis suureks väljakutseks eelkõige algoritmide arendajatele, rakendajatele ja regulaatorile.

Profiilanalüüsiga kaasnevad teatud riskid üksikisiku põhiõigustega hõlmatud privaatsusele. Need riskid seostuvad eelkõige diskrimineerimise, isikliku identiteedi kaotamise (ingl *de-individualisation*) ja informatsiooni asümmeetriaga ehk vastukäivusega (ingl *information assymetries*).[128] Diskrimineerimise risk avaldub siis, kui ennustavad algoritmid õpetavad iseennast diskrimineerida kallutatud andemete põhjal, mis on näiteks seotud isiklike omandustega nagu rahvuslik kuuluvus, sugu, usk, vanus jm.[129] Automatiseeritud süsteemid võivad otsuste või ennustamiste tegemiseks kaevandada ka palju ebatäpset või erapooletut informatsiooni sisalduvaid andmekogumeid, millest on lõppkokkuvõttes tingitud puudulikud ennustused ja hinnangud, seades kahtluse alla süsteemi õigluse.[130]

Isikliku identiteedi kaotamist põhjustab eelkõige otsustusprotsess, kus isikuid hinnatakse eelkõige konkreetse grupi omaduste põhjal, mitte iga isiku kohta individuaalsete tunnuste põhjal.[131] Teabe asümmeetriaga on kokkupuudet olukorras, kus püstitatud eesmärgiks on saama võimalikult rohkem ülevaadet andmesubjektidest, kuna andmed annavad väärtuslikke ressursse ja teadmisi neile, kes omavad ja kasutavad andmeid.[132] Eelnimetatud profiilanalüüsist tulenevad riskide esinemist saab põhjendada eeskätt sellega, et algoritmid ei suuda ise inimmõistuse tasandil filtreerida või kontrollida tõele vastavust või eluliselt usutavust talle analüüsimiseks antud andmeid või informatsiooni. Profiilanalüüsi riskid ei pruugi autori seisukohal alati kõik korraga realiseerida eriti juhul, kui profiilanalüüsi koostamine toimub ühe isiku andmete põhiselt näiteks hoolsusmeetmete kohaldamise raames isiku riskiprofiili

[128] Schermer, B. W. The limits of privacy in automated profiling and data mining. – Computer Law & Security Review 2011/27, No.1, lk 46. – https://doi.org/10.1016/j.clsr.2010.11.009 (18.04.2021).
[129] *Ibidem,* lk 47.
[130] Politou, E. Alepis, E. Patsakis, C. Profiling tax and financial behaviour with big data under the GDPR. – Computer Law & Security Review 2019/35, No. 3, lk 308. – https://doi.org/10.1016/j.clsr.2019.01.003 (18.04.2021).
[131] Schermer, lk 47.
[132] *Ibidem.*

koostamine, kus võetakse analüüsiks usaldusväärsetes avalikes registrites kuvatud teave ja kohustatud isikule kliendi poolt edastatud andmed.

Üldjuhul profiilanalüüsi koostamisel peavad andmed olema täpsed, õiged ja kehtivad tagamaks otsuse usaldusväärsust. Tehisintellekti süsteemi arendajal ega rakendajal ei pruugi olla teadmist, et analüüsiks kasutatavad andmed võivad olla vigased. Seega ka süsteemi lõppkasutajat peaks puudutama kohustus kontrollida, uuendada enda isikuandmeid ja vajadusel nõuda teenuste pakkujatelt andmete parandamist. Tehisintellekti selgitatavuse nõue võib tegelikult minimiseerida profiilanalüüsist johtuvaid riske, kuid see eeldab, esiteks, kõigi osapoolte arusaama tehisintellekti süsteemi toimuvatest protsessidest, tagajärgedest ja ohtudest, võimalust sekkuda süsteemi vältimaks diskrimineerivaid otsuseid üksikisikute suhtes, ning teiseks, andmete kvaliteet ja õigsus peab samaaegselt tagama selle protsessi tulemuslikkus.

Euroopa Liidu tasandil on läbipaistvus omanud suurt tähtsust juba viimased kolmkümmend aastat, kasvades välja vastusena puudulikule legitiimsusele ja probleemidele, mis tuleneb demokraatia defitsiitsusest. Kuigi läbipaistvus rakendub erinevates valdkondades erinevalt, kuid ühisena keskse mõttena on tegemist läbipaistmatuse ja salatsemise vastandiga.[133] Kantuna sissejuhatuses püstitatud uurimisküsimusest lahatakse järgmises alapeatükis IKÜM-i regulatsioonist tuleneva läbipaistvuse põhimõtte võrdväärsust tehisintellekti süsteemi läbipaistvusega. Üheselt pole võimalik sedastada, kas see regulatsioon suudab tagada isikuandmete töötlemisel tehisintellekti läbipaistvust.

Läbipaistvus on üheks andmekaitse aluspõhimõtteks, mis tuleneb IKÜM artiklist 5, moodustades koos seaduslikkuse ja õiglusega esimese taolise alusreegli, mida võib nimetada viimaseks võimaluseks kindla olukorra lahendamiseks, kui muud täpsemad põhimõtted ei rakendu.[134] Läbipaistvus saab defineerida kui midagi, mis on selge, ilmne ja kahtlematult ning üheselt arusaadav.[135] Füüsilist isikut puudutavate isikuandmete kogumine, kasutamine, lugemine või töötlemine ja nende töötlemise ulatus praegu või tulevikus peaks olema nende

[133] Karageorgu, V. Transparency principle as an evolving principle of EU law: Regulative contours and implications. – https://www.right2info.org/resources/publications/eu-karageorgou-vasiliki-transparency-principle-as-an-evolving-principle-of-eu-law/view (10.04.2021).
[134] Felzmann, H. Villaronga, E. F. Lutz, C. Tamo-Larrieux, A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. – Big Data & Society 2019, lk 2. – https://journals.sagepub.com/doi/pdf/10.1177/2053951719860542 (10.04.2021).
[135] EK C-110/03, *Belgia Kuningriik versus komisjon*, ECLI:EU:C:2005:223, kohtujurist D. Ruiz-Jarabo Colomer ettepanek, p 44.

jaoks läbipaistev. See eeldab, et isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Andmesubjekte tuleb teavitada eelkõige vastutava töötleja identiteedist ning töötlemise eesmärgist ning muust teabest, mis peaks tagama asjaomaste füüsiliste isikute suhtes õiglane ja läbipaistev töötlemine. Lisaks on andmesubjektidel õigus saada neid puudutavate isikuandmete töötlemise kohta kinnitust ja sõnumeid. Teavitada tuleks veel isikuandmete töötlemisega seotud ohtudest, normidest, kaitsemeetmetest ja õigustest ning sellest, kuidas nad saavad sellise andmete töötlemisega seonduvalt oma õigusi kaitsta.[136]

Viidates IKÜM artikli 12 lõikele 1 viimane nõuab, et vastutav töötleja teavitab andmesubjekti „isikuandmete töötlemisest kokkuvõtlikult, selgelt, arusaadavalt ning lihtsasti kättesaadavas vormis, kasutades selget ja lihtsat keelt," eriti tuleb sellega arvestada, kui teave on suunatud konkreetselt lapsele. Teave on kokkuvõtlik ja selge juhtudel, mil vastutav töötleja esitab andmesubjektile vastava teabe efektiivselt ja lühidalt, eristades selgelt muust andmesubjektile esitatavast teabest, nt lepingutingimustest tulenev muu teave või kasutusjuhendid. Interneti keskkonnas saab vastutav töötleja seda tagada n-ö kihtide loomisega, kus on selgelt välja toodud vajalik informatsioon, mis eristub ja pole seotud muude tingimustega.[137]

Teave on arusaadav juhul, kui sellest saab aru keskmise teadmistega isik andmesubjektide hulgas, kelle isikuandmeid töödeldakse. Sellest tulenevalt on arusaadavus kontekstist sõltuv ning vastutustundlik vastutav töötleja peab tagama, et just konkreetne andmesubjektide ring saab esitatavast teabest aru, ja rakendama meetmeid, et vajalik teave esitatakse konkreetselt neile arusaadaval kujul.[138] Teabe kergesti kättesaadavust tuleb tõlgendada kitsalt, andmesubjektile ei tohi olla kohustatud vastavat teavet otsima, vaid see peab olema talle koheselt arusaadav, mil viisil ja kohas see on talle kättesaadav, nt andes teabe otse andmesubjektile, lisades viite juba võimaliku taotluse täitmisele, viidates sellele küsimuse vormis vastavas alajaotuses „vt". Näitlikustamiseks peaks interneti lehekülgedel, mis isikuandmeid koguvad ja töötlevad konkreetne alajaotus, nt „Privaatsussätted", mille avades on

[136] IKÜM, põhjendus 39.
[137] The Article 29 Working Party. Guidelines on Transparency under Regulation 2016/679, WP260, lk 7. – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227&fbclid=IwAR08HU1Akd29jRoWMzlFJq2cOQZ1_Rz6ldclrKmI9TAE-ah5809C7er1Bjw (21.04.2021).
[138] *Ibidem*, lk 7.

andmesubjektil võimalik seda teavet saada, miks, kuidas ja mis eesmärgil tema isikuandmeid töödeldakse[139]

Andmesubjektile tuleb teave esitada kasutades nii lihtsat keelelist vormi kui võimalik edastamaks kiirelt ja efektiivselt põhisõnum, vältides keerulisi keelelisi konstruktsioone, liigseid tehnilisi termineid ja lauseehituslikke võtteid ning jättes kõrvale võimalusi erinevatele tõlgendamistele.[140] Läbipaistvuse põhimõtte puhul on võimalik eristada kaht elementi: ettevaatavust (ingl *prospective*) ja tagasivaatavust (ingl *retrospective*). Ettevaatav läbipaistvus seisneb selles, et andmesubjekti tuleb teavitada isikuandmete töötlemisest enne, kui see töötlemine algab.[141] Ettevaatav läbipaistvus eeldab, et vastutav töötleja edastab andmesubjektile teavet enda (kes?), töödeldavate andmete kvaliteedi ja hulga (kuidas?), töötlemise ajaraami (millal?), töötlemise põhjuse (miks?) ja töötlemise eesmärgi (mille jaoks?) kohta.[142] Eelkõige teatud olulist teavet on vastutav töötleja kohustatud ennetavalt andmesubjektile esitama.[143] Tagasivaatav läbipaistvus peab tekitama võimaluse aru saamaks, kuidas ja miks kindel otsus vastu võeti.[144]

Läbipaistvuse vaatepunktist tuleb eelkõige tagada, et andmesubjektile ei tuleks isikuandmete töötlemise ulatus üllatusena, vaid tal peab olema võimalus enne töötlemist aru saada, mis määral ja tagajärgedega isikuandmete töötlemine toimub.[145] Tavaliselt organisatsioonidel on heaks tavaks sätestada vastav teave eraldatuna üldtingimustest nn kliendiandmete töötlemise põhimõtetes, milles tehakse avalikult kättesaadavaks isikuandmete töötlemisega seonduvat teavet, mis annaks andmesubjektile ehk kliendile õiguse tutvuda, milliseid andmeid kogutakse ja töödeldakse, mis alusel ja eesmärgil seda tehakse. See tõstab usaldustunnet organisatsiooni vastu ja võimaldab vajadus pöörduda isiku andmeid töödeldava organisatsiooni poole nii andmete uuendamiseks, parandamiseks või kustutamiseks kui ka laiemalt õigusrikkumistest teavitamiseks ja nende lõpetamiseks. Nende puhul tuleb siiski silmas pidada, et antud

[139] Article 29 Working Party, WP260, lk 7-8.
[140] *Ibidem*, lk 8-10
[141] Felzmann (jt), lk 3.
[142] *Ibidem.*
[143] The Council of Europe. Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series - No. 223. Strasbourg, 2018, lk 12. – https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (21.04.2021).
[144] Felzmann (jt), lk 3.
[145] Article 29 Working Party, WP260, lk 7.

eesmärgid oleksid juba algselt kooskõlas andmekaitse põhimõtetega ja andmeid ei kogutaks igaks juhuks taoliselt, et see ei täida eesmärgipärast tegevust.

Organisatsiooni tegevusetuse korral on andmesubjektil võimalik seega nõuda tema õiguste kaitsmist väljaspool organisatsiooni näiteks eskaleerida asja Andmekaitse Inspektsiooni või kohtu poole. Vastavate asutuste poole pöördumisel on veelgi enam tähtis, et otsuste vastuvõtmine on olnud piisaval määral läbipaistev. Õiguskaitseorganite poole pöördumise efektiivsuse tagamisel on vajalik sedastada, kuidas vastavad otsused vastu võeti või mille tõttu antud mõjud avaldusid.

Tuginedes varasemalt kirjutatule, et tehisintellekti läbipaistvus eeldab eelkõige tehisintellekti süsteemidest arusaamist, nendel süsteemidel põhinevate otsuste ja ennustuste tegemise arusaadavust ja jälgitavust ning hõlmab ka analüüsitavate andmete kvaliteeti, et inimene suudaks selgitada algoritmide loogikat, kuidas jõuti igal konkreetsel juhul järeldusele või millistel kaalutlustel oli tehtud vastav otsus. Viimane tähendab tehisintellekti süsteemi arendaja või rakendaja suutlikkust teavitada puudutavaid andmesubjekte ja laiemalt avalikkust süsteemide otsuste tegemise protsessidest. Seega tehisintellekti läbipaistvus seostatakse selgitatavuse põhimõttega. Isikuandmete töötlemise kontekstis kohustab üldmääruse artiklis 12 sätestatud läbipaistvuse põhimõte vastutavat töötlejat kasutusele võtta meetmeid, mis võimaldavad andmesubjekti teavitada isikuandmete töötlemisega seonduvatest toimingutest, sh automatiseeritud töötlusel põhinevate üksikotsuste ja profiilanalüüsi tegemise loogikast, sellise töötlemise tähtsusest ja ennustatavatest tagajärgedest andmesubjekti jaoks tulenevalt üldmääruse artiklist 13 lõike 2 punktist f ja artiklist 14 lõike 2 punktist g koosmõjus artikli 22 lõigete 1 ja 4.

Üldmäärus loetleb küll toiminguid ja tegevusi, mille kohta tuleb andmesubjekti teavitada, kuid ei määratle lähemalt meetmeid, mida tuleb vastutaval töötjal kasutusele võtta täitmaks nimetatud teavitamise nõue. Üldmäärus nendib, et tootjaid tuleks julgustada isikuandmete töötlemisel põhinevate või enda ülesannete täitmiseks isikuandmete töötlevate toodete, teenuste ja rakenduste väljatöötamisel ja kavandamisel arvestama andmesubjekti õigusega andmekaitsele ja tagama teaduse ja tehnoloogia viimast arengut arvestades, et vastutavad töötlejad ja volitatud töötlejad suudaksid täita oma andmekaitsealaseid kohustusi.[146]

[146] IKÜM, põhjendus 78.

Samas ei tulene üldmäärusest, kuidas süsteemide tootjate ja arendajate n-ö innustamine peab tegelikult välja nägema, et kõnealuse sidusrühma esindajad saaksid sätestatu ellu viia, sealjuures tagades vastutavatel ja volitatud töötlejatel võimaluse täita üldmäärusest tulenevaid nõudeid. Seega üldmäärus määrab kohustuse teavitada ka isikuandmete töötlemisel põhineva või enda ülesannete täitmiseks isikuandmete töötleva rakendusena tehisintellekti süsteemide ja protsesside loogikast, sh prognoositavatest tagajärgedest, kuid ei anna otseselt juhiseid, kuidas täita seda kohustust ka tehisintellekti süsteemide suhtes tagamaks vähemalt tehisintellekti rakendamisel isikuandmete töötlemise läbipaistvust.

Sellest tulenevalt saab isikuandmete kaitse üldmääruse läbipaistvuse põhimõtet pidada liiga üldiseks, et seda oleks võimalik efektiivselt rakendada tehisintellekti süsteemidele ja nende poolt vastu võetud otsustele. Võrdväärse läbipaistvuse tagamiseks on eelkõige vajalik tehisintellekti süsteemide edasine reguleerimine, hõlmates selle põhilisi tunnuseid ja nendest tulenevaid riske.

2. TEHISINTELLEKTI SÜSTEEMIDE REGULEERIMISE VAJADUS LÄBIPAISTVUSE SAAVUTAMISEKS

2.1. Tehisintellekti süsteemide regulatsiooni lähtekoht

Tehisintellekti süsteemid on kiirelt arenev tehnoloogia valdkond, mille laialdase rakendamise läbi on võimalik saavutada nii majanduslik kui ka sotsiaalne areng. Selle puhul tuleb mõista, et tehisintellekti süsteemid hakkavad meie igapäevaelule järjest enam mõju avaldama, olenemata sellest, kas me seda sisuliselt tajume või mitte. Tehisintellekti ümbritseb ühiskondlikult teatav kahtlusefoon, mida on läbi aastate aidanud tekitada erinevad käsitlused populaarkultuuri teostes, mis võivad olla liialt dramaatilised. Sellegipoolest, ei saa tähelepanuta jätta, et taolised süsteemid on keskmisele inimesele väga arusaamatud ja nende kasutamisel võivad ohtu sattuda meie põhiõigused ja vabadused. Järgnevates lõikudes on toodud ära tehisintellekti süsteemide regulatsiooni lähtekoht, ehk millised suuremad murekohad võivad vajada täiendavat reguleerimist.

Üldmäärus ei reguleeri otsesõnu tehisintellekti kasutamist isikuandmete töötlemisel, kuid mitmed selle sätted omavad tehisintellekti osas suurt tähtsust. Sarnaselt pakub tehisintellekti võimalused andmete töötlemisel suurt väljakutset osadele kehtivatele sätetele ja põhimõtetele. Sellegipoolest tuleb suuta ühildada ja arendada olemasolevaid põhimõtteid tehisintellekti võimalusi ja eeliseid arvesse võttes.[147]

Tehisintellekt ja selle poolt tehtud otsused võivad olla tavainimese mõistes liiga keerulised, et neid sisuliselt mõista, kuid see ei tähenda, et süsteem, mis on keeruline, ei peaks olema samal ajal läbipaistev. Õiguskirjanduses on väljendatud seisukohta, et tehisintellekti läbipaistvuse tagamisele on mitmed kitsaskohad, mis võivad muuta reguleerimise küll formaalselt teostatavaks, kuid mis sisuliselt ei aita otsesõnu andmesubjektide õiguste kaitsele kaasa.[148]

Tehisintellekti algoritmid on võimalik teha formaalselt läbipaistvaks avaldades algoritmi koodi. Taoline avaldamine on täpselt nii kasulik, kui paljud inimesed sellest sisuliselt aru saaksid.

[147] Sartor/Lagioia, lk II.
[148] Temme, M. Algorithms and Transparency in View of the New General Data Protection Regulation. – European Data Protection Law Review (EDPL) 2017/3, No. 4, lk 476.

Samas polekski läbipaistvuse saavutamiseks tingimata vajalik viimsestki süsteemi detailist aru saada. Sellest tähtsam on aru saamine kontseptsioonist, kuidas ja miks ning milliste vahenditega tehisintellekti otsuste vastuvõtmisesse rakendatakse.[149] Üheks võimaluseks läbipaistvusele kaasa aitamiseks on muuta algoritmid tõlgendatavaks, mis tähendab, et avalik oleks viis, kuidas tehisintellekt kasutatavate andmetega suhtleb ja mida täpsemalt kasutab.[150] Vajalikke teadmisi kontseptsiooni tasandil on võimalik saavutada läbi erinevate viiside, kuid see eeldaks ühtset ja läbimõeldud lähenemist nii avaliku kui erasektori poolt, hõlmates ühiskonda laiendatult.[151]

Tehisintellekti üheks omaduseks on selle põhimõtteline läbipaistmatus. Algoritmide liigne kitsendamine ja teadmatuse sihipärane vältimine võib liigselt takistada selle tööd ja eesmärkide täitmist. Algoritmide keerulisuse ja nende kasutusvõimaluste vahel on korrelatsioon, mis tähendab, et reguleerimise tulemusel puuduks n-ö sobilikel algoritmidel kasulikkus.[152] Samas tuleb tõdeda, et ükski süsteem ei ole üles ehitatud ja rakendatud täielikus teadmatuses, kuidas see toimib. Suurema läbipaistvuse ja kontrollimise võimaluse saavutamiseks tulekski vastavad võimalused süsteemi juba seda arendades lisada. Taoliste läbipaistvust suurendavate mehhanismide lisamine juba valmis süsteemile võib kujuneda peaaegu võimatuks või anda ainult pealiskaudset kasu.[153]

Raskuskoht võib seega ilmneda juba kasutusele võetud tehisintellekti süsteemides, mida kasutatakse tänapäeval isikuandmete töötlemisel, sh profiilanalüüsi koostamisel. Sellest tulenevalt peab kohustulikus korras olema tagatud võimalus inimesel sekkuda tehisintellekti süsteemi enne automatiseeritud lõppotsuse või ennustuse tegemist ja/või hinnata taoliste otsustuste või ennustuste adekvaatsus ja tõele vastavus võttes arvesse parameetrid, millest tehisintellekt on oma analüüsis lähtunud, ja tausta informatsioon konkreetse isiku kohta ehk temaga seotud elulised asjaolud, st kas tehtud otsus või ennustus läheb nende asjaoludega kokku või mitte.

[149] Temme, lk 476,
[150] Stoyanovich, J. Goodman, E. P. Revealing Algorithmic Rankers. – Freedom to Tinker 2016. – https://freedom-to-tinker.com/2016/08/05/revealing-algorithmic-rankers/ (27.04.2021).
[151] Temme, lk 476-477.
[152] *Ibidem*, lk 477.
[153] Kroll, J. A. Huey, J. Barocas, S. Felten, E. W. Reidenberg, J. R. Robinson, D. G. Yu, H. Accountable Algorithms. – University of Pennsylvania Law Review 2017/165, No.3, lk 637. – https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review (12.04.2021).

Tähelepanuta ei saa jääda ka algoritmide poolt kasutatavate andmete kvaliteet, mille kogumisel võivad juba kaasneda eelarvamuslikud riskid. Sellise juhul võimendub algoritmi võimalus teha otsuseid, mis ei ole seaduspärased või eetilised. Teabel on erinevad väärtused olenevalt selle kasutusvaldkonnast, sama andmehulk võib erinevas otsustusprotsessis päädida täielikult erinevate väljunditena.[154] Tehisintellekti poolt andmete töötlemisel võivad kaasneda juba olemasolevad diskrimineerivad mõjud, mis algoritmi toimel võimenduvad juhuslikult.[155] Eelkõige tulebki minimaliseerida taoliste tendentside teke andmete kogumise ja töötlemise algfaasis, sest hiljem võib tehisintellekt neid andmeid kasutades jõuda otsusteni, mis tuginevad valedel alustel.

Algoritmilist otsustusprotsessi rakendavad paljud eraettevõtted, erilist riski kätkevad endast taolised andmesubjekti märkimisväärselt mõjutada võivad otsused nagu krediiditaotluste lahendamine. Krediidiasutustega kaasneb problemaatika just ärisaladusega seonduvalt. Ärisaladusest tulenevalt võivad andmete töötlejad olla teadlikult vastumeelsed rakendamaks sisulist läbipaistvust tagavaid meetmeid. Läbipaistmatus on seega viis, kuidas ettevõtte huve kaitsta erinevate teiste osapoolte eest, kelleks võivad olla andmesubjektid, valitsused või konkurendid. Ärisaladuse kaitseks ja piisava läbipaistvuse saavutamiseks saab rakendada erapooletuid entiteete, mis seisavad nii läbipaistvuse kui ka ärisaladuse kaitse eest.[156]

Tehisintellekti reguleerimine pole kergete killast ülesanne, kätkedes endas nii hetkeolukorda kui ka laiemat vaadet tulevikku. Regulatsioon peab olema piisav selleks, et nii tagada andmesubjektide õiguste piisav kaitse kui ka tehnoloogia areng ja selle kiirus. Sellegipoolest ei saa edasi liikuda ilma sisulise regulatsioonita, kuna tulenevalt tehisintellekti olemusest võib see endas sisaldada märkimisväärset riski paljudele turuosalistele.

[154] Temme, lk 478.
[155] Barocas, S. Selbst, A. D. Big Data's Disparate Impact. – California Law Review 2016/104, No. 3, lk 674. – https://www.jstor.org/stable/24758720 (12.04.2021).
[156] Temme, lk 479-480.

2.2. Tehisintellekti reguleerimise kavatsus Euroopa Liidu õiguses

2021. aasta aprilli lõpus avalikustati Euroopa Parlamendi ja nõukogu määruse ettepanek[157], mille eesmärgiks on paika panna Euroopa-ülene lähenemine tehisintellektile. Sellest saaks esimene tehisintellekti reguleeriv õigusraamistik, mis kätkeb endas tehisintellekti riskide maandamist eesmärgiga tagada Euroopa globaalne juhtroll antud valdkonnas. Käesolevas alapeatükis analüüsitakse antud ettepaneku suuremaid pidepunkte, mis seonduvad tehisintellekti läbipaistvusega tagamisega.

Laiemalt on kavandatava määruse eesmärgiks tagada Euroopa ühisturul kasutatavate tehisintellekti süsteemide turvalisus ja vastavus liidu väärtustele ja põhimõtetele. Tehisintellekti tehnoloogia arendamise ja rahastamise seisukohast on määrava tähtsusega selle valdkonna esmane reguleerimine ja teatava õigusselguse loomine. Lisaks sellele aitab kavandatav määrus suurendada valdkonna suhtes juba kehtivate õigusaktide efektiivsust ja peaks suutma välistada ühisturu killustumist.[158] Ohuks võib pidada olukorda, kus vastavad süsteemid on Euroopa Liidu liikmesriikides erinevalt reguleeritud, mis tekitaks segadust nii tarbijates, tootjates ja arendajates.

Tehisintellekti süsteemid taoline reguleerimine paneb kohustused kõrge riskiga tehisintellekti süsteemide pakkujatele ja kasutajatele. Pakkujatele loob regulatsioon kindluse, et nende poolt loodavad tehisintellekti süsteemid, mis vastavad antud nõuetele, oleksid ühisturul vabalt kaubeldavad ja piiride ülene tegevus poleks takistatud. Ettevõtetele, mis kasutavad tehisintellektist lähtuvaid võimalusi, tagab see suurema tarbijatepoolse usalduse.[159]

Regulatsioon on üles ehitatud riskipõhisele lähenemisele, mis peaks tagama, et regulatsioon ei muutuks liigseks takistuseks tehisintellekti tehnoloogia arendamisele või selle rakendamise majanduslikule mõttekusele, vältides sellega ülereguleerimist laiemalt. Riskipõhiselt on võimalik tuvastada tehisintellekti süsteeme, mille kasutamine kindlaks eesmärgiks omab kas vastuvõetamatut riski, kõrget riski või madalat riski.[160] Vastuvõetamatu riskiga on eelkõige

[157] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, COM/2021/206 final. Brussels, 21.04.2021. – https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (24.04.2021).
[158] *Ibidem*, lk 3.
[159] *Ibidem*, lk 10.
[160] *Ibidem*, lk 12.

viisid, mil tehisintellekti kasutatakse eesmärgiga manipuleerida inimeste käitumisega ja muuta seda sellises suunas, mille kaudu avaldub füüsiline ja/või vaimne vägivald sellele või mõnele muule inimesele.[161] Vastuvõetamatu riskiga tehisintellekti süsteemid tulenevad kavandatava määruse artiklist 5, milles sedastatakse tehisintellekti kasutamise keelatus. Sarnaselt eeltoodule on keelatud avaliku sektori poolt rakendatavad tehisintellekti süsteemid, mis annavad inimestele nende sotsiaalse käitumise, teadaoleva või ennustatava käitumismalli järgseid hindeid või tasemeid vastavalt nende usaldusväärsusele, millel võib olla märkimisväärne negatiivne mõju konkreetsele isikule või isikute grupile.[162]

Tehisintellekti on keelatud õiguskaitseorganite poolt kasutada reaalajas kaugelt juhtivalt avalikus kohas toimuva biomeetrilise identifitseerimise protsessi käigus, kui see just ei ole rangelt piiritletud erandlikel eesmärkidel. Lubatud on see vaid juhtudel, mil selle abil üritatakse tuvastada konkreetseid võimaliku kuriteo ohvreid, k.a kadunud lapsi, mil selle abil üritatakse ennetada konkreetset, märkimisväärset ja peatselt toimuvat ohtu füüsilise isiku elule või tervisele või terroriakti, mil seda kasutatakse kindlate kuritegude toimpanemises kahtlustatavate isikute avastamiseks, lokaliseerimiseks, isikusamasuse tuvastamiseks või kohtu alla andmiseks.[163]

Tehisintellekti kasutamine sellistel eesmärkidel on selgelt tugeva puutumusega inimeste privaatsusesse, õigustesse ja vabadustesse, ning selle rakendamisel tuleb tagada selle tegevuse proportsionaalsus ning ajaline ja ruumiline piiratus.[164] Üldjuhul on lubatud tehisintellekti taoliseks tegevuseks rakendada vaid sõltumatu avaliku võimu asutuse või kohtu loal. Kavandatav määrus jätab liikmesriigile võimaluse täiendavalt siseriiklikult reguleerida, millistel juhtudel on lubatud tehisintellekti süsteemi taoliseks tegevuseks rakendada.[165] Määruse mõjualast jäävad välja tehisintellekti süsteemid, mida arendatakse ja kasutatakse eksklusiivselt ainult sõjaväeliste asutuste poolt.[166]

[161] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 16.
[162] *Ibidem,* artikkel 5 (1c).
[163] *Ibidem*, artikkel 5 (1d).
[164] *Ibidem*, põhjendused 18-20.
[165] *Ibidem*, artikkel (3-4).
[166] *Ibidem*, põhjendus 12.

Käesoleva magistritöö kontekstis omavad kõige suuremat puutumust kõrge riskiga valdkonnad ja nendes rakendatavad tehisintellekti süsteemid. Kõige huvipakkuvam regulatsioon on kavandatava määruse artiklis 6 (kõrge riskiga tehisintellekti süsteemide klassifikatsioon), artiklis 7 (lisa III muudatused), artikkel 13 (läbipaistvus ja kasutajatele esitatav teave), artikkel 14 (inimese poolt teostatav järelevalve), ning artikkel 15 (täpsus, robustsus ja küberturvalisus).

Tehisintellekti süsteem on eelkõige kõrge riskiga juhtudel, mil see langeb määruse artikli 6 mõjualasse, loetledes kõrge riskiga tehisintellekti klassifikatsioonide põhimõttelised alused. Kõrge riskiga tehisintellekti süsteemid peaksid olema lubatud ainult siis, kui need vastavad kindlaks määratud nõuetele. Nõuete eesmärgiks peab olema, et kõrge riskiga tehisintellekti süsteemid ei kujutaks vastuvõetamatut ohtu tähtsatele avalikele huvide.[167] Täpsem valdkondlik määratlus on toodud kavandatava määruse lisas III, millest tulenevalt loetakse tehisintellekti süsteem kõrget riski omavaks näiteks juhtudel, mil seda kasutatakse tööhõives, töötajate haldamiseks või juurdepääsuks füüsilise isikuna ettevõtjaks olemiseks,[168] hariduses või kutsete saamisel,[169] juurdepääsu tagamiseks olulistele era- või avaliku sektori teenustele või hüvitistele,[170] korrakaitses individuaalsete riskianalüüside koostamisel,[171] või seonduvalt migratsiooni, asüüli taotluste või piirkontrolli teostamisega.[172]

Esimesel juhul tuleneb kõrge risk asjaolust, et vastav valdkond mõjutab otseselt inimeste karjäärivõimalusi ja elus toimetulekut, ning see peaks olema rakendatav mis iganes töötamise viisile, võttes arvesse muudatusi töötamise vormides. Vastavas valdkonnas on kõrge risk teatavate nõrgalt kaitstud sotsiaalsete gruppide diskrimineerimisele.[173] Pole keeruline ette kujutada olukorda, kus valedel alustel või andmetel otsuseid tegev tehisintellekti süsteem mõjutab märkimisväärselt indiviidi karjäärivõimalusi või välistab need juba eos. Tööhõive valdkond on viimastel aastatel olnud kiires arengus ja tingimused, mis omavad tähtsust varasemalt võivad olla ebavajalikud juba praegu või lähitulevikus. Tehisintellekti süsteemi

[167] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 27.
[168] The European Commission. ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council, COM/2021/206 final. Brussels, 21.04.2021, Annex III, lk 4. – https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (27.04.2021).
[169] *Ibidem,*
[170] *Ibidem.*
[171] *Ibidem,* lk 4-5.
[172] *Ibidem,* lk 5.
[173] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 36.

rakendamisel taoliste otsuste tegemisel tuleb arvestada neid tingimusi kogumis võrreldes kehtivale arusaamale ja eetikale.

Teisel juhul tuleneb risk olukorrast, kus läbi ebaõige tehisintellekti süsteemi rakendamise võib indiviidil tekkida suured raskused saada juurdepääsu erinevatele haridust pakkuvatele asutustele, mis raskendab tema edasist elu ja võimalusi.[174] Indiviidi ligipääs haridusele on üheks määravaimaks aspektist tema edasises elus, pannes aluse mitmetele protsessidele ja trendidele. Haridusest tulenevad mõjud on kõikehõlmavad ja need on paljuski ennustamatud. Eelkõige tuleb tagada, et nendega seonduvad otsused on tehtud õiglastel ja asjakohastel alustel, mis on kooskõlas indiviide põhiõiguste ja vabadustega.

Kolmandal juhul tuleb arvestada asjaoluga, et tegemist on kriitiliste teenustega, milleta on raskendatud indiviididel tavapäraselt enda elu korraldada, nt eluase, kommunaalteenused, toetused jne.[175] Kriitiliste teenuste nimekiri on viimastel aastatel laienenud. Elu toimub järjest enam virtuaalseid kanaleid kasutades, mis kätkeb endast suuremat riski läbipaistmatute otsuste tegemisel ja nende hilisemal põhjendamisel. Inimsekkumiseta tehtavad otsused, mis omavad kohest mõju indiviidi toimetulekule, võivad olla kaalutlusvigadega, arvestamata olukorra spetsiifilisi ja indiviidist tulenevaid aspekte.

Neljandal juhul tuleb arvestada, et korrakaitseasutused on eelduslikult juba jõupositsioonil, mille puhul tekib risk selle positsiooni kuritervitamisele. Juhtudel, mil tehisintellekti süsteem ei treenitud piisava kvaliteediga andmetega, ei vasta kehtestatud nõuetele, võib selle tegevus muutuda kiirelt diskrimineerivaks. Olukordades, mil tehisintellekti süsteemi tegevus ei ole piisavalt läbipaistev, selgitatav ja dokumenteeritud, võib tekkida risk isikute õigusele ausale kohtupidamisele, süütuse presumptsioonile ja muudele tema põhiõigustele.[176] Valedel alustel tehtud riskihinnang võib isiku elu mõjutada aastaid pärast õigusrikkumiste sooritamist, võides saada aluseks edasistele piirangutele ning karistustele.

Viiendal juhul on tegemist isikutega, kes on põhimõtteliselt haavatavas seisus ning nende saatus paljuski sõltub pädevate avalike ametiasutuste otsustest. Otsuste vastuvõtmisel tuleb tagada

[174] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 35.
[175] *Ibidem*, põhjendus 37.
[176] *Ibidem,* põhjendus 38.

tehisintellekti süsteemi täpsus, diskrimineerimise vaba toimimine ning nende laiapõhjaline läbipaistvus. Põhiõigused, mis võivad saada ebaõigete otsuste tõttu kannatada on õigus vabale liikumisele, eraelu ja isikuandmete kaitsele, rahvusvahelisele kaitsele ja heale haldustavale.[177] Otsused, mis tehakse rahvusvahelist kaitset vajavate isikute suhtes, omavad laiapõhjalist mõju nii nende kui ka teiste inimeste elus, omades puutumust meie põhiarusaamale elu olulisusest ning selle kaitse tähtsusest.

Kõrge riskiga tehisintellekti süsteemide nimekiri on toodud lahtiselt, jättes võimaluse seda täiendada vastavalt vajadusele, tagades läbi selle regulatsiooni paindlikkuse.[178] Lisas III toodud nimekirja on võimalik täiendada juhul, kui on täidetud kaks tingimust. Esiteks peab tehisintellekti süsteemi kasutuseesmärk langema lisas III toodud alajaotuste alla, ning teiseks peab see kujutama ohtu isikute tervisele, turvalisusele, või omama riski kahjulikuks mõjuks isikute põhiõigustele.[179] Taolise riski sisustamisel tuleb silmas pidada uue tehisintellekti süsteemi eesmärki, selle kasutamise ulatust või planeeritavat ulatust, selle puhul juba avaldunud kahjulikku mõju, selle kahjuliku mõju edaspidi avaldumise ulatust ning palju muud.

Tehisintellekti süsteemide poolt kasutatavad andmehulgad peavad olema kõrge kvaliteediga, eriti juhtudel, mil neid kasutatakse tehisintellekti süsteemi treenimisel erinevate mudelite loomisel, mida kasutatakse edaspidi üksikotsuste vastuvõtmisel. Süsteemi eesmärgist lähtuvalt peavad andmehulgad olema relevantsed, iseloomulikud, vabad suurematest vigades ja täielikud. Diskrimineerimise vältimiseks peab andmehulga kujundamisel arvestama konkreetsete taustsüsteemidega, mis võivad tulenevad nii geograafilisest piirkonnast, käitumismallidest või funktsioonikirjeldusest. Vältida tuleb olukorda, mil tehisintellekti süsteem muutub erapoolikuks või isegi diskrimineerivaks tulenevalt ebapiisava kvaliteediga andmetest või mudelistest.[180]

Andmete kvaliteet seondub tugevalt eelpool toodud otsuste vastuvõtmisega, sest vead algandmetes võivad tekitada olukorra, kus automatiseeritud süsteem jõuab järeldusele, mis pole

[177] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 39.
[178] *Ibidem,* artikkel 7.
[179] *Ibidem,* artikkel 7 (1).
[180] *Ibidem*, põhjendus 44.

põhimõtteliselt korrektne. See kõik eeldab, et ennekõike on vajalik tagada andmete kogumise ulatuse ja töötlemise õiguspärasus ning andmekogude faktiline tõesus igas ajahetkes.

Kavandatava määruse artikkel 13 sätestab tehisintellekti süsteemide läbipaistvuse põhimõtte ja kasutajatele pakutava teabe ulatuse. Kõrge riskiga tehisintellekti süsteemid tuleb kavandada ja arendada sellisel viisil, mis tagaks nende tööprotsessidest piisava arusaadavuse, andes kasutajatele võimaluse tõlgendada selle tulemust ja seda korrektselt kasutada.[181] Lisaks on vajalik tagada kasutusjuhendite olemasolu, milles sisalduv teave on kokkuvõtlik, täielik, õige ja selge, mis on kasutajaid silmas pidades asjassepuutuv, kättesaadav ja arusaadav.[182] Nendes materjalides peab muuhulgas sisalduma teave tehisintellekti identiteedi osas, kontaktandmed ja vajadusel tema volitatud esindaja identiteet ja kontaktandmed. Tehisintellekti süsteemi osas on vajalik välja tuua selle töötamise omadused, võimekused ja piirangud. Selles sisalduvad tehisintellekti süsteemi kavandatav eesmärk; selle täpsusaste, robustsuse ja küberturvalisuse tase, mille osas on läbi viidud adekvaatne testimine; teadaolevad või ennustatavad tingimused, mis võivad viia riskide realiseerumisele; selle tegevus seondudes isikutega või isikute gruppidega, kelle suhtes süsteemi kavandatakse rakendada; kui vajalik, milliseid andmehulki süsteemi testimisel ja valideerimisel on kasutatud. Samuti muudatused tehisintellekti süsteemi, mis on toimunud pärast selle turule paiskamist, inimese poolt teostatava järelevalve meetmed, ning tehisintellekti süsteemi eeldatav elutsükkel, vajalikud hooldus- ja korrashoiumeetmed, mis tagavad selle korrektse toimise.[183]

Eelpool mainitu on aluseks, et tagada tehisintellekti süsteemide läbipaistvus, kuid see on võimalik vaid juhul, kui kõikidel osapooltel on olemas teadmised ja oskused selliste andmete tõlgendamiseks. Prioriteetide nimekirjas peab olema kõrgel kohal just teadlikkuse ja vastava hariduse laiendamine, et riske maandavad meetmed ei kehtiks vaid formaalselt.

Minimaliseerimaks riski indiviidide tervisele, turvalisusele või põhiõigustele, mis võib tuleneda kõrge riskiga tehisintellekti süsteemi kasutamisel, tuleb süsteem kavandada ja arendada selliselt, et sellele on võimalik efektiivselt teostada inimese poolt järelevalvet. Seda aitavad tagada kaks meedet. Esimese meetme puhul on inimese poolt teostatava järelevalve võimalus

[181] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, artikkel 13 (1).
[182] *Ibidem*, artikkel 13 (2).
[183] *Ibidem*, artikkel 13 (3).

korrektselt tuvastatud ja tehisintellekti süsteemi sisseehitatud enne, kui see turule paisatakse. Teisel juhul on järelevalve võimalus korrektselt tuvastatud ja vajadusel rakendatav kasutaja enda poolt.[184]

Johtuvalt oma eesmärgist peab tehisintellekti süsteem olema piisaval määral täpsed, robustsed ja turvalised. Süsteemi täpsusaste tulenevalt konkreetsetest väärtustest tuleb määratleda sellega kaasnevates juhendites. Kõrge riskiga süsteemidel peab olema kõrge töökindlus, mida saab tagada läbi erinevate meetmete, näiteks korrektne varundamine, süsteemivigade kiire tuvastamise ja protsesside sisulise kontrollimise. Taoline süsteem peab olema vastupidav igasugustele väljapoolt tulevate rünnakute vastu, võttes arvesse täpseid riske, mis töötlemisega kaasnevad.[185] Kõrge küberturvalisuse tase tuleb eelkõige tagada põhjusel, et tehisintellekti süsteemide vastastel erinevatel rünnetel võib olla suur mõju selle töökindlusele ja otsuste läbipaistvusele. Kui rünnaku tulemusel muutuvad süsteemi aluspõhimõtted või kasutatavate andmete hulk või väärtus, võib olla väga keeruline tuvastada, mis alusel otsused tehti.[186]

Tehisintellekti süsteem, mida põhimõtteliselt ei peeta kõrget riski omavaks, võib vajada läbipaistvuse tagamiseks sellegipoolest täiendavat spetsiifilist regulatsiooni. Silmas tuleb pidada, et süsteemid, mis suhtlevad füüsiliste isikutega, võivad kätkeda endas konkretiseeritavat riski isikusamasuse tuvastamisel või pettuste tuvastamisel. Kuigi need süsteemid ei pea langema määruse mõistes kõrget riski omavate süsteemide klassifikatsiooni, tuleb taoliste süsteemide kasutamisel füüsilist isikut vähemalt teavitada, et suhtlus toimub tehisintellekti süsteemiga, kui see just pole ilmselge tulenevalt suhtluse viisist või tingimustest. Teavitamisel tuleb arvestada erinevate inimrühmade võimalustega saada vajalikku informatsiooni neile sobivas vormis või formaadis.

Tehisintellekti süsteemide kasutajad, kes rakendavad süsteemi audiovisuaalse materjali loomiseks või muutmiseks selliselt, et tulemus sarnaneb pärismaailmas olevale isikule, kohale või sündmusele, ning mille puhul poleks võimalik keskmisel inimesel aru saada, et tegemist on valeinfoga, peavad vastava materjali märgistama selliselt, et oleks võimalik aru saada, et tegemist pole tõese teabega vaid tehisintellekti poolt loodud kujutisega.[187] Sellest tulenevalt,

[184] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, artikkel 14 (1-3).
[185] *Ibidem*, artikkel 15 (1-4).
[186] *Ibidem*, põhjendus 51.
[187] *Ibidem,* põhjendus 70.

kuigi regulatsioon on sihitud kõrge riskiga tehisintellekti süsteemide reguleerimisele, peab olemasolevaid nõudeid silmas pidama ka muude süsteemide rakendamise või kasutamise korral, lähtudes nendes ilmnevate riskide ulatusele ja võimalikele tagajärgedele.

Eelpool mainitud madala riskiga tehisintellekti süsteemid ei lange antud kavandatava määruse reguleerimisalasse, sellegipoolest tuleks nende kasutuselevõtmisel määruses toodud regulatsiooniga mõistlikul määral arvestada. See võib luua suuremat usaldusväärsuse fooni tehisintellekti süsteemide vastu üldiselt ja aitab kaasa süsteemide kasutuselevõtmisele ning rakendamisele. Madala riskiga tehisintellekti süsteemide loojaid ja kasutajaid innustatakse looma vastavasisulisi tegevuseeskirju, milles lepitakse kokku ühtsed lähenemised taoliste süsteemide rakendamisel.[188]

Määruse üheks eesmärgiks on tagada, et õiguslik regulatsioon ei saaks takistuseks tehisintellekti süsteemide arendamisele või kavandamisele. Selle eesmärgi saavutamiseks tuleb turuosalistele viia läbi erinevates formaatides teavitusi ning seada üles võimalusi turvalises keskkonnas süsteeme arendada ja testida. Regulatsioon ei tohiks pärssida innovatsiooni, vaid peab piiritlema ja konkretiseerima reeglid, mille läbi on võimalik tehisintellekti süsteeme turvaliselt arendada väljaspool nende rakendamist, enne kui need füüsilistele isikutele mõju jõuavad avaldada. Vastavate keskkondade regulatsioon kätkedes endas nii raamistikku, milles need tegutsevad, kui ka suhtlust järelevalvega peab olema ühetaoline, tagamaks ühetaolist rakendamist üle kogu Euroopa.[189]

Kavandatav määrus sedastab põhjalikult, mis valdkondades ja kuidas on vajalik tehisintellekti süsteeme reguleerida, et tagada nende läbipaistvus, ja vältida ning maandada riske füüsilistele isikutele, kui neid rakendatakse. Antud loetelu on regulatsiooni mastaapi arvestades lahtine ja peaks selle läbi võimaldama paindlikku lähenemist, mis ei tohiks raskendada tehisintellekti süsteemide arendamist ja kasutuselevõtmist. Määruse sõnastusest võib järeldada, et põhiline rakendatav meede läbipaistvuse tagamiseks on ennetamisele suunatud. Tehisintellekti süsteemid tuleb juba arendada ja ehitada selliselt, et need vastaksid liidu väärtustele ja põhiõigustele, mis peaks märkimisväärselt lihtsustama nende edasist kasutamist ja vastavust regulatsioonile mõttele. See kindlasti pole lihtne ülesanne, kuid arvestades tehisintellekti

[188] The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, põhjendus 81.
[189] *Ibidem*, põhjendused 71-72.

süsteemide omadusi, oleks märkimisväärselt keeruline selle vastavust kehtestatud nõuetele muude lahendustega. Selline lähenemine paneb regulatsiooni põhirõhu tehisintellekti süsteemide arendajatele, kes peavad eelkõige saama aru selle eesmärkidest ja toimimise põhimõtetest.

Võideldes tehisintellekti süsteemile igiomase läbipaistmatuse vastu, tuleb kasutajatele tagada adekvaatsete kasutusjuhendite olemasolu, mis annaks sisulise võimaluse tõlgendada tehisintellekti poolt vastu võetud otsuseid või muid asjaolusid. Sellegipoolest ei saa tähelepanuta jätta antud süsteemide edasist toimimist ja tõhusat kontrolli nende üle. Kavandatav regulatsioon koostoimes isikuandmete kaitse üldmääruses sätestatuga peaks olema piisav, et tagada andmesubjektide põhiõiguste ja vabaduste kaitse juhtudel, mil isikuandmeid töötleb tehisintellekti süsteem. Arvestades regulatsiooni uudsust ja veel selgusetut rakenduspraktikat, vajab antud teema veel täiendavat analüüsi. Just viimasest kooruvad välja uue regulatsiooni nõrkused ja tugevused.

2.3. Tehisintellekti reguleerimine Eesti õiguses läbipaistvuse saavutamiseks

Sarnaselt Euroopa Liidu seadusandlusele on Eestis kavas välja töötada eraldiseisev õiguslik regulatsioon, mille eesmärk on reguleerida algoritmilisi e tehisintellekti süsteeme tervikuna. Uue seaduse väljatöötamise kasuks räägivad asjaolud, et taolisi süsteeme on erinevaid ja nendest tulenevad riskid pole alati võrreldavad. Sarnaselt kavandatavale Euroopa Parlamendi ja nõukogu määrusele tuleks eristada madala riskiga süsteeme ja kõrge riskiga süsteeme. Regulatsiooni eesmärk oleks panna paika reeglid just kõrge riskiga süsteemidele, milleks on muuhulgas erasektoris rakendatavad süsteemid, mille otsustel on üksikisiku õiguste seisukohast õiguslikud või sellega samaväärselt olulised tagajärjed, märkimisväärse varalise või mittevaralise kahju oht; oht elule või tervisele või mille tagajärgi füüsilised isikud ei saa mõistlikkuse piires vältida.[190] Kõrgema riskiga süsteemide määratlemisel saab eelduslikult juhinduda kavandatava määruse tõlgendusest, mis on enda definitsioonist laia rakendusalaga ja paindlik.

[190] Krati VTK, lk 23-25.

Väljatöötamise kavatsus viitab mitmetele juhtumitele, mil vead tehisintellekti süsteemis on toonud kaasa märkimisväärsed mõjud füüsilistele isikutele. Taolistest süsteemides on tuvastatud vigu, mis on toonud kaasa hinnangute tegemise, mis on olnud eelarvamuslikud, stereotüüpsed ning kallutatud. Probleemiks ongi kujunenud otsuste tõlgendamine, mille puhul pole otsuseid vastuvõtvad asutused hiljem suutnud selgitada, kuidas ja millistel alustel need vastu võeti.[191] Piisava läbipaistvuse korral oleks olnud võimalik sellistes olukordade teket vältida või suuremal määral takistada. Sellistest olukordadest tuleneb, et tehisintellekti süsteemid võivad omada juba praegu meie elu üle suurt kontrolli, kuigi teadlikkus nendest otsustest võib olla võrdlemisi madal.

Läbipaistvuse saavutamise viisidena tuuakse välja eelkõige teavitamise tähtsust. Teavitama peab üksikisikut eelkõige juhtudel, kui inimesega suhtleb inimesele sarnane algoritmil põhinev dialoogisüsteem; kõrgema riskitasemega algoritmilise süsteemi puhul tuleb eelnevalt teavitada algoritmi aluseks olevast otsustusprotsessi loogikast, millised on selle juures isikuandmete töötlemise tähtsus ja tagajärjed; samuti peab indiviid teavitama IKÜM artiklis 22 lõikes 3 sätestatud kaitsemeetmetest.[192] Lähtuvalt tehisintellekti süsteemide läbipaistmatusest osutub hetkel teavitamine algoritmi otsustusprotsessi loogikast problemaatiliseks selle protsessi täieliku arusaamise puudumise tõttu nii kasutuselevõtjate kui ka arendajate poolt.

Eelpool toodust tulenevalt poleks regulatsiooni eesmärk kehtestada nõudeid madala riskiga algoritmilistele süsteemidele, millest kerkib küsimus, kuidas ja millises ulatuses tõlgendada erasektoris kasutatavaid süsteeme kõrget riski omavateks isikuandmete töötlemise suhtes. Tavaline arusaam nendest on seotud veebipõhiste krediidiotsustega ja veebipõhine tööle värbamine ilma inimsekkumiseta[193], kuid praktika kindlasti laiendab antud loendit.

IKÜM artiklis 22 toodud nõuded kehtivad vaid eritingimustel ja tulenevalt tehisintellekti reguleerimisest tulenevaid väljakutseid võivad sealsed nõuded jääda ebapiisavaks, et läbipaistvust tagada. Erandid reeglitest on laialdased ja isegi näiline inimsekkumine välistaks nende rakendamise sootuks. Eeltoodust tulenedes tuleks rõhku panna inimsekkumise

[191] Krati VTK, lk 3-4.
[192] Krati VTK, lk 26.
[193] IKÜM, põhjendus 71.

laiapõhjalisele reguleerimisele, et tagada selle sisuline rakendamine, mille võimalikkus on otsustusprotsessis läbiv ja autoriteetne.

Läbipaistvust on võimalik saavutada taoliste sekkumise võimaluste süsteemi lisamisega juba selle arendusfaasis, mis peaks suutma tagada süsteemi muutmise võimalust ka hiljem, kui regulatsioon või selle rõhuasetus muutuvad. Selleks on vajalikud konkreetsed reeglid ja juhised, mida on efektiivselt võimalik rakendada. Põhirõhuks tuleb riigisiseselt seada selgitustöö, millistest alustest lähtub tulevane regulatsioon ja selle vajalikkus ning eesmärk. Reguleerimise mõte ei tohi olla takistada tehnoloogia arengut ja laiemat konkurentsivõimet antud valdkonnas. Seda enam, et Eesti ei tohiks jääda ülereguleerimise tõttu kõrvale võimalustest, mis antud süsteemide kasutamine ja rakendamine võiks endaga kaasa tuua. Pole ebatõenäoline, et riikides, mis lähevad väiksema reguleerimise teed, saavad selge konkurentsieelise ja võivad edaspidi dikteerida valdkonna laiemat pilti ja arengut.

Regulatsiooni mõjud on laiapõhjalised. Avaliku võimu asutused saavad automatiseeritud süsteeme rakendades järjest enam keskenduda sisulisemat analüüsi vajavatele küsimustele, vähendades sellega märkimisväärselt halduskoormust. Tuleb arvestada, et igakülgse reguleerimise tulemusel tõuseb algselt erinevate asutuste töökoormus, et viia protseduurid ja olemasolevad süsteemid vastavusse kehtima hakkava regulatsiooniga. Suuremaks eesmärgiks peab siiski olema efektiivsuse kasv nii avalikus kui ka erasektoris. Uute süsteemide arendamisel on põhipingutuseks läbipaistvuse tagamine algusest peale, mis paneb suurema koormuse arendajatele, kuid peaks neile samas kinnitama, et nende toode või toote osa vastab nõuetele ja selle kasutamine on kooskõlas meie kõigi õiguste ja vabadustega.[194] Erilist puutumust omab regulatsioon asutustele ja ettevõtetele, mis juba praegu kasutavad laialdaselt tehisintellekti süsteeme teatavate otsuste vastuvõtmisel.

Kavandatava Euroopa Parlamendi ja nõukogu määruse valguses ja selle arengujärgust tulenevalt on raske määratleda, millisel kujul on Eesti õiguses tehisintellekti süsteeme vajalik ja võimalik reguleerida, kuid see ei tähenda, et antud küsimuse analüüsiga ei saaks või ei peaks riigisiseselt edasi liikuma. Vähemalt osaliselt sedastab kavandatav määrus liikmesriigi õigust ja kohustust kehtestada eraldiseisvat regulatsiooni, nt keelatud tehisintellekti süsteemide kasutamisel avalikus kohas jälgimiseks. Prevaleerivaks võib hoopis kujuneda ühiskondlik

[194] Krati VTK, lk 29-31.

debatt, millisel kujul ja millistel eesmärkidel on mõistlik kasutada tehisintellekti süsteeme. Kaaluda tuleb nii positiivseid tulemusi kui ka negatiivseid, viimastel puhul tuleb rakendada neist tulenevaid õpikogemusi, et tõhustada protseduure ja luua turvalisem rakendusala.

Olles tehisintellekti reguleerimise lähtekohal, tuleb arvestada, et tulevikuperspektiiv on võrdlemisi ebaselge. Süsteemselt on vajalik tagada regulatsiooni paindlikkus ning ühiskonnagruppide teadlikkus kasv, võimaldades nii arendada ning pakkuda turvalisi tehisintellekti lahendusi, mis omavad positiivset mõju laiemale inimkonna arengule.

KOKKUVÕTE

Tehisintellekti süsteemide kasutamine on muutunud peaaegu lahutamatuks osaks hulgaliste isikuandmete töötlemisel nii era- kui ka avalikus sektoris. Sellel on kokkupuude erinevate indiviidide ja erinevate ühiskonnagruppidega. Eelkõige saab neid süsteeme pidada kasulikeks, mille eesmärgiks on suurendada erinevates tööprotsessides kiirust, efektiivust ning töökindlust. Sellegipoolest võivad tehisintellekti poolt tehtud otsused olla läbipaistmatud või lausa diskrimineerivad. Kantuna asjaolus, et tehisintellekti kasutamine võib kaasa tuua isikute põhiõiguste ja vabaduste piiramise, on valdkonna edasise reguleerimise vajadus ilmne.

Käesoleva magistritöö uurimisprobleemiks oli tehisintellekti läbipaistmatusest tulenev risk isiku kohta ebasoodsate ja ootamatute järelduste tegemisel profiilianalüüsi koostamisel või muude automatiseeritud otsuste vastuvõtmisel.

Sellest tulenevalt oli magistritöö eesmärgiks välja selgitada, mil määral tehisintellekti rakendamisel isikuandmete töötlemisel profiilianalüüsis on võimalik täita isikuandmete kaitse üldmääruses sätestatud läbipaistvuse põhimõtet; ning kindlaks määrata, millised õiguslikud nõuded ja meetmed tagavad piisaval määral tehisintellekti süsteemide kaasamise abil isikuandmete töötlemise läbipaistvust.

Magistritöö eesmärgist tulenevalt käsitleti lähemalt tehisintellekti süsteemide kategoriseerimist ning võimalikku tulevikuperspektiivi. Selgitati välja, millisel määral on tehisintellekti süsteemide läbipaistvus võrdeline isikuandmete kaitse üldmääruses sätestatud läbipaistvuse põhimõttega. Järgnevalt tuli arutluse alla kas ja kuidas on võimalik tagada tehisintellekti algoritmidel põhineva isikuandmete töötlemise läbipaistvus ilma selle otsustusprotsessi inimese poolt sekkumata. Veel enam, kas ainult tehisintellekti protsessidest arusaamisest piisab, et tagada isikute põhiõiguste efektiivne kaitse. Viimasena analüüsiti, millistele nõuete peab tehisintellekti süsteemide läbipaistvus vastama isikuandmete töötlemisel tulevikuperspektiivis.

Tehisintellekti süsteemid on viimastel aastatel teinud läbi märkimisväärse arengu. Sellegipoolest pole tehisintellekti mõiste üldteada või osutub teadmine vaid pinnapealseks. Euroopa Komisjon defineerib tehisintellekti kui tarkvarapõhiseid või virtuaalmaailmas tegutsevaid või riistvarasse paigaldatud süsteeme, mis käituvad intelligentselt, analüüsivad

ümbruskonda ja teostavad teatavas ulatuses iseseisvaid toiminguid konkreetsete eesmärkide saavutamisel. Käesoleva magistritöö mõttes tuleb tegemist kitsa tehisintellekti mõistega, see suudab täita piiratud rida ülesandeid. Enamik kasutusel olevaid tehisintellekti süsteeme langevad just sellesse kategooriasse. Masinõpet peetakse tehisintellekti aladistsipliiniks, mille omapära seisneb varasemate kogemuste kasutamises tulemuste parandamiseks või täpsete ennustuste tegemiseks. Masinõppe erinevaid vormid on kõige suurema puutumusega antud teemasse ja põhilisteks vahenditeks, mille abil isikuandmeid töödeldakse.

Profiilianalüüsiks on IKÜM-i kohaselt igasugune isikuandmete automatiseeritud töötlemine, mis hõlmab isikuandmete kasutamist füüsilise isikuga seotud teatavate isiklike aspektide hindamist. Profiilianalüüs ja muud automatiseeritud üksikotsuste vastuvõtmine eeldab, et neid toiminguid tehakse ilma inimsekkumiseta. Profiilianalüüs ja muud automatiseeritud üksikotsuste vastuvõtmine on reguleeritud IKÜM artiklis 22, mille kohaselt on taoliste otsuste vastu võtmine, mis toob füüsilisele isikule kaasa teda puudutavaid õiguslikke tagajärgi või muid märkimisväärseid mõjusid, üldjuhul keelatud. Sellegipoolest on regulatsioonis toodud mitmed erandid, mille kohaldamisel tuleb olla ettevaatlik, et mitte kanduda kõrvale isikuandmete kaitse põhimõtetest. Tehisintellekti kasutamisel on vastuvõetud otsused tehtud ilma inimsekkumiseta ja seega langevad need antud artikli mõjualasse.

Tehisintellekti süsteemidele on omane põhimõtteline läbipaistmatus. Taoline läbipaistmatus komplitseerib potentsiaalsete õigusrikkumiste tuvastamist ning tõendamist, vastutuse omistamist, kahjunõuete esitamise tingimuste täitmist ja õigusmõistmisele juurdepääsu tulemuslikkust negatiivse mõjuga otsuste puhul. Selle läbipaistvuse käsitlus taandub sellele, kuidas saab mõõta, selgitada ning põhjendada andmete ja algoritmide sünergiat tehisintellekti süsteemides vältimaks seeläbi andmesubjekti suhtes võimalikke negatiivseid tagajärgi. Tehisintellekti läbipaistvus seondub eelkõige selgitatavuse põhimõttega, hõlmates endas andmete, ärimudelite ja protsesside läbipaistvust, süsteemide suutlikkusest ja otstarbest avalikku teavitamist ning otsuste arusaadavust ja jälgitavust.

Tehisintellekti läbipaistvuse nõue on üks olulisemaid eetikapõhimõttel tuginevatest nõuetest, mida tuleb täita kogu selle elutsükli jooksul. Autori hinnangul ei piisa tehisintellekti süsteemide läbipaistvuse tagamiseks isikuandmete töötlemisel ja nende põhjal profiilianalüüsi koostamisel ning muude üksikotsute vastuvõtmisel IKÜM-is leiduvast läbipaistvuse põhimõttest, olles

selleks eesmärgiks liialt üldine, vaid selle läbipaistvuse saavutamiseks on vajalik tehisintellekti edaspidine reguleerimine, võttes arvesse just nende süsteemidega kaasnevaid riske ning ülesehitust.

Tehisintellekti süsteemide reguleerimine pole olnud lihtne ülesanne. Regulatsiooni lähtekohaks on tänane reaalsus, kus tehisintellekti süsteeme rakendatakse paljudes valdkondades ja sageli meile arusaamatul kujul. Tehisintellekti reguleerimisel omavad eelkõige tähtsust selle läbipaistvuse saavutamise keerulisus, sellele vastupidiselt omane läbipaistmatus ning selle poolt kasutatavate andmete kvaliteet. Reguleerimise muudab raskemaks kaalutlused, mille kohaselt võib liigne reeglite kehtestamine pärssida antud sektori arengut ning Euroopa konkurentsivõimet laiemalt.

Valdkonna laiahaardeliseks reguleerimiseks on koostatud Euroopa Parlamendi ja nõukogu määrus, mille eesmärgiks on ühest küljest tehisintellekti süsteemidest tulenevate riskide maandamine, tagades füüsiliste isikute põhiõiguste ja vabaduste kaitse, teisest küljest õigusselguse loomine, et tagada valdkonna jätkusuutlik areng ning efektiivsus. Määruse vormis reguleerimine aitab tagada regulatsiooni ühetaolisuse terves Euroopa Liidus, tagades selle läbi ühisturu efektiivse toimimise ja vältides sellega õiguslikku killustumist.

Kavandatavas regulatsiooni põhialuseks on riskipõhine lähenemine, mille toimel sedastatakse regulatsiooni sihtrühm, milleks on kõrge riskiga tehisintellekti süsteemid. Vastav määratlus aitab vältida ebavajalikku reguleerimist süsteemide osas, mis omavad füüsilistele isikutele vähest mõju või madalat riski. Vastuvõetamatut riski sisaldavad tehisintellekti süsteemid keelatakse või nende rakendamisvõimalustele kehtestatakse märkimisväärsed piirangud ja nõuded.

Eraldiseisvalt keskendub kavandatav määrus tehisintellekti läbipaistvuse saavutamisele. Selle põhialuseks on ennetav lähenemine. Tehisintellekti süsteemid tuleb juba arenduse ja loomise käigus viia kooskõlla kindlate nõuetega, mis peaks tulevikus tagama, et nende tööprotsessidest oleks võimalik piisavalt aru saada ning saadud tulemusi pädevalt tõlgendada ja efektiivselt kasutada.

Süsteemid tuleb varustada kasutusjuhenditega, milles sisalduv teave peab olema kokkuvõtlik, täielik, õige ja selge, ning mis on kasutajaid silmas pidades asjassepuutuv, kättesaadav ning arusaadav. Materjalides peab muuhulgas sisalduma teave tehisintellekti pakkuja identiteedi kohta, tema kontaktandmed. Tehisintellekti osas tuleb sedastada selle töötamise omadused, võimekused ning piirangud. Lisaks tehisintellekti süsteemi kavandatav eesmärk, selle täpsusaste, robustsuse ning küberturvalisuse tase, ning palju muud. Kasutusjuhendist tulenevalt peaks kasutajal tekkima laiapõhjaline arusaam tehisintellekti süsteemi toimimisest ja tööpõhimõtetest, mille abil on võimalik selle osas tõhusat järelevalvet teostada. Vastavasisulise nõude täitmine eelduslikult ei taga täielikult tehisintellekti läbipaistvust, kuid aitab sellele selgelt kaasa. Prioriteetide nimekirjas peab olema veel ühiskonna teadlikkuse ja vastava hariduse laiendamine, et vastavad riske maandavad meetmed ei kehtiks ainult formaalselt. Tehisintellekti süsteemide arendamisel ja loomisel tuleb rõhku panna võimalustele, et selle üle oleks võimalik teostada inimese poolt sisulist järelevalvet.

Tehisintellekti poolt kasutatavad andmehulgad peavad olema kõrge kvaliteediga, ning lähtuvalt selle eesmärgist olema relevantsed, iseloomulikud, vabad suurematest vigadest ja täielikud. Diskrimineerimise vältimiseks peab andmehulga kujundamisel arvestama erinevate infoväljadega, mis avaldavad nende tõlgendamisel sisulist tähtsust. Juhul, kui andmed ei vasta neile nõuetele, ei saa välistada, et isegi nõuetele vastav tehisintellekti süsteem suudaks vastu võtta sisuliselt õigeid otsuseid. Andmete kogumise ulatus ja töötlemise õiguspärasus ning andmekogude faktiline tõesus tuleb tagada läbivalt.

Kavandatava määruse reguleerimise mõjualast jäävad välja madala riskiga tehisintellekti süsteemid. Sellegipoolest on soovitatav, et taolised süsteemid järgiksid samuti nõudeid, mis on kohustuslikud kõrge riskiga süsteemidele. Selline määratlus eeldab analüüsimist, milliseid mõjusid või riske võivad taolised süsteemid endas peita ning vajalikud meetmed kasutusele võtta. Kuna kavandatavas regulatsioonis on kõrge riskiga tehisintellekti süsteemide määratlus toodud lahtiselt, ei saa välistada, et algselt madala riskiga süsteem võib tulevikus langeda hoopis kõrge riskiga kategooriasse. Lisaks tuleb arvestada, et igasugused vabatahtlikud meetmete kasutuselevõtmised aitavad kindlasti kaasa usaldusväärsuse kasvule, millel on positiivsed mõjud kogu sektorile.

Autor leiab, et kavandatava määruse regulatsioon koostoimes IKÜM-i vastavasisulise regulatsiooniga on piisav, et tagada tehisintellekti süsteemide läbipaistvus, isegi juhtudel, mil süsteemi otsustusprotsessis puudub inimese poolt sekkumine täielikult. Sellegipoolest tuleb tagada tehisintellekti süsteemide vastavus kehtestatud nõuetele ning eraldi rõhku tuleb panna juba loodud süsteemide uuendamisse ning avalikkuse teadlikkuse kasvatamisse. Läbipaistvuse saavutamiseks on põhialuseks just ennetav tegevus, mille abil on võimalik tulevikus veel keerulisematest süsteemidest aru saada. Protsessidest arusaamisele peab lisanduma muude nõuete täitmine, et tehisintellekti süsteemid ei muutuks haavatavaks võimalikele rünnetele või vigadele, mis ajas võivad kumuleeruda.

Sarnaselt Euroopa Liidu seadusandlusele on Eestis kavas välja töötada tehisintellekti süsteeme käsitlev seadus, mille eesmärgiks on reguleerida tehisintellekti süsteeme tervikuna. Oma sisulist ja lähtekohast seondub see tugevalt kavandatava määrusega ning annab võimaluse vajadusel määruse regulatsiooni täpsustada. Eraldi rõhutatakse seaduse väljatöötamise kavatsuses teavitamise tähtsust, mille kaudu on võimalik maandada tehisintellektist tulenevaid riske. Kavandatava Euroopa Parlamendi ja nõukogu määruse valguses on veel vaja välja selgitada, millisel kujul ja määral on vajalik tehisintellekti süsteemide edaspidine reguleerimine Eesti õiguses. Siseriiklikult omab suuremat tähtsust selgitustöö tegemine, millisel kujul ning millistel eesmärkidel on mõistlik vastavaid süsteeme kasutada.

Kavandatava regulatsiooni mõjud on laiapõhjalised tuues kaasa suurema võimaluse tehisintellekti süsteemide rakendamisele ning kasutamisele. Juba tehisintellekti süsteeme kasutavad avaliku ja erasektori asutused saavad juurde kindlust, et nende tegevus vastab kehtivatele nõuetele. Regulatsiooni kehtima hakkamise algfaasis tuleb sellegipoolest arvestada asjaoludega, et olemasolevate süsteemide nõuetele vastavusse viimine suurendab töökoormust, kuid eesmärgistatud tegevuse korral ei suuda see protseduure liigselt negatiivselt mõjutada. Avaliku sektori asutused saavad automatiseeritud süsteeme rakendades järjest enam keskenduda sisulisemat analüüsi vajavatele küsimustele, see aitab kaasa protsesside efektiivsemaks muutumisele ning halduskoormuse vähendamisele.

Magistritöö analüüsist selgus, et tehisintellekti kasutamisel profiilianalüüsi koostamisel või muude automatiseeritud üksikotsuste vastuvõtmisel kannab endast märkimisväärset riski füüsiliste isikute põhiõigustele ning vabadustele. Läbipaistmatuse probleemi lahendamiseks

tuleb kehtestada mitmeid nõudeid, mille alusel on võimalik riske maandada. Protsessi läbipaistvust on võimalik saavutada lähtudes spetsiaalsetest nõuetest, mida kavandatav määrus tehisintellekti süsteemidele kehtestab. Need nõuded koos muude meetmetega tagavad tehisintellekti süsteemide läbipaistvuse piisaval määral, kuid tuleb arvestada, et nõuete täitmise üle tuleb pidada efektiivset järelevalvet ning tõsta inimeste teadlikkust antud valdkonnas. See kõik eeldab laiapõhjalist ning kõikehõlmavat lähenemist. Tuleb tõdeda, et arvestades regulatsiooni värskust, eeldab probleemipüstitus veel lähemat analüüsi, kui selguvad selle rakendamisega seonduvad kitsaskohad ning võimalikud raskused.

THE CONFORMITY OF THE PROCESSING OF PERSONAL DATA USING ARTIFICIAL INTELLIGENCE WITH FUNDAMENTAL PRINCIPLE OF TRANSPARENCY SET OUT IN THE GENERAL DATA PROTECTION REGULATION. Abstract

Nowadays, artificial intelligence technology has become an integral part of the processing of personal data in the private and public sectors. It helps organisations process data in substantial volumes, save time and human resources by automating the processes, and generating or making decisions, etc. However, artificial intelligence systems in processing personal data should comply with the General Data Protection Regulation (from now on, GDPR). The data protection regulation applies to manual personal data processing and the automated processing of personal data. As artificial intelligence systems in personal data processing are considered automated processing, the GDPR requirements on personal data protection apply to such processing.

The topic of this master's thesis is relevant to the fact that the processing of personal data by artificial intelligence algorithms may, as a result of their automated decision-making and profiling, lead to adverse or unforeseen decisions or predictions on a particular person. In the light of automated processes, the question arises of how to ensure artificial intelligence transparency in these cases. The European Commission's White Paper on Artificial Intelligence highlighted the problems caused by the lack of transparency of artificial intelligence. The last makes it challenging to control compliance with existing European Union legislation to protect fundamental rights, ensure the effectiveness of law enforcement, and access justice for the decisions that could negatively impact natural persons. Furthermore, there may not be sufficient means for controlling how the decision or prediction has been made using artificial intelligence algorithms.

The research problem of the master's thesis is the risk arising from the opacity of artificial intelligence for making unfavourable and unexpected decisions on a person in a profile analysis. Artificial intelligence algorithms can teach themselves, so the algorithm's parameters may change during a learning process. In this case, the algorithm developer may not always explain relationships between variables are taken into account in the classification of the algorithm or at which stage of the algorithm it occurs, or determine exactly how the algorithm constructs different relationships between variables to achieve the result. Thus, the involvement of

artificial intelligence in the processing of personal data may lead to a situation where artificial intelligence algorithms derive a conclusion from a large set of data in the framework of a profile analysis, which may have adverse effects or consequences for the particular person. As a result, there are problems in ensuring the protection of the individual's fundamental rights and calling into question the reliability and legality of the derived decision.

First of all, the purpose of the master's thesis is to find out whether it is possible to comply with the principle of transparency laid down in the GDPR when applying artificial intelligence in the processing of personal data in profile analysis. Secondly, this thesis aims to determine which legal requirements and measures will ensure sufficient transparency of the processing of personal data through the use of artificial intelligence systems.

Due to the research problem and purposes of the master's thesis, the following research questions have been identified:

- Which are the most common artificial intelligence systems in use?
- To what extent is the requirement for transparency in artificial intelligence equal to the principle of transparency laid down in the GDPR?
- Is it possible to ensure the transparency of the processing of personal data based on artificial intelligence algorithms without human intervention in this technical process? How can it be guaranteed?
- Is the understanding of artificial intelligence processes alone sufficient to ensure the protection of the fundamental rights of natural persons?
- What requirements should transparent artificial intelligence comply with when processing personal data?

In the master's thesis, the qualitative and analytical methods have been used to solve the main research problem, achieve the previously set purposes, and conclude the aforementioned research questions. Specifically, the master's thesis is a qualitative study, but the author uses an analytical method to achieve the purposes. Using a qualitative method stems from the need to analyse the principle of transparency stipulated in the GDPR theoretically in the context of the transparency of artificial intelligence. The analytical method has been applied to study the literature required for this thesis, including defining the concepts under the GDPR and the technical side of artificial intelligence. The author primarily uses literature and scientific articles

in English, especially in writing chapters regarding artificial intelligence. The sources in English are preferable in this thesis as theoretical and legal issues related to artificial intelligence are thoroughly covered in research articles and works published in English. As the master's thesis topic is closely related to personal data processing and, more generally, data protection, the European Union General Data Protection Regulation prevails in examining the conformity of AI transparency with the principle of transparency. Besides, in the master's thesis, the author uses the intention of the Estonian Ministry of Justice on working towards regulation on the algorithmic systems` effects and relevant guidelines of the European Commission on approach for artificial intelligence and the Article 29 European Independent Working Party set up by the European Data Protection Board.

Artificial intelligence systems have gone through rapid development in recent years. Nevertheless, the concept of artificial intelligence is not well-known by the public. The European Commission defines artificial intelligence systems as software, something that is active in the virtual world or wired into the hardware, which acts intelligently and performs tasks independently to achieve its purpose. The thesis looks at artificial intelligence systems that are considered to be narrow in their performance. Most of the artificial intelligence systems currently deployed belong to this category. Machine learning is a subdiscipline of narrow artificial intelligence, which uses its previous experiences to streamline work processes or makes accurate predictions. These different forms of machine learning systems are mostly linked to this thesis and the primary systems used to process personal data.

In GDPR, profiling means any form of automated processing of personal data consisting of personal data to evaluate certain personal aspects relating to a natural person. Profiling and other automated individual decisions are made without human intervention. These kinds of processing are further regulated in GDPR Article 22, which purports that decisions based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject, is by default prohibited. The article offers different exceptions to the general prohibition, but these exceptions must be considered further, not to infringe the data subjects rights and freedoms. Decisions made by artificial intelligence systems are, by definition, done without human intervention.

Artificial intelligence systems are in their nature opaque, which complicates discovering potential trespasses and gathering evidence in situations where the artificial intelligence systems negatively affect a natural person. The approach to transparency comes down to how the synergies between data and algorithms in artificial intelligence systems can be measured, explained, and justified to avoid possible negative consequences for the data subject. The transparency of artificial intelligence relates to the principle of clarity, including the transparency of data, business models and processes, public communication of the capabilities and purpose of systems, and the comprehensibility and traceability of decisions. The requirement of transparency of artificial intelligence is one of the essential ethical requirements that must be met throughout its life cycle. In the author's eyes, the principle of transparency depicted in the GDPR is not enough to ensure the transparency of artificial intelligence systems in the processing and profiling personal data and other individual decisions because its regulation is too general. Further regulation of artificial intelligence systems is necessary to achieve required transparency, taking into account the risks and structure of these systems.

Regulating artificial intelligence systems is not an easy task. The starting point for the regulation is today's reality, where artificial intelligence systems are applied in many different areas and in a form that is often incomprehensible to us. The complexity of achieving its transparency, the inherent opacity of the systems and the quality of the data it uses are significant in regulating artificial intelligence. Regulation is made more difficult by considering that excessive regulation may hamper the development of the sector and European competitiveness as a whole.

Proposal for a Regulation of the European Parliament and of the Council has been drawn up to regulate the sector comprehensively to mitigate the risks arising from artificial intelligence systems, ensure the protection of fundamental rights and freedoms of natural persons, and create legal clarity to ensure sustainable development and efficiency. Regulating these systems in this way helps to ensure regulatory uniformity throughout the European Union, thereby ensuring the effective functioning of the common market and avoiding legal fragmentation. The proposed regulation is based on a risk-based approach and targets high-risk artificial intelligence systems. This definition helps to avoid unnecessary regulation of systems that have little or no risk to individuals. Artificial intelligence systems containing an unacceptable risk shall be prohibited or subject to significant restrictions and requirements.

Separately, the proposed regulation focuses on achieving transparency in artificial intelligence systems. It is based on a proactive approach. Artificial intelligence systems must be brought into line with specific requirements during development and creation, ensuring that their work processes can be adequately understood. The results obtained can be interpreted competently and used effectively.

High risks systems must be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and precise information that is relevant, accessible and understandable to users. Concerning the artificial intelligence system, the characteristics, capabilities and limitations of its operation must be stated. In addition, the intended purpose of the AI system, its level of accuracy, robustness and cybersecurity, and much more. As a result of the instructions for use, the user should have a broad understanding of the operation and operating principles of the artificial intelligence system, which will allow effective monitoring. Compliance with this requirement presumably does not fully ensure the transparency of artificial intelligence but contributes to its development. The list of priorities must also include raising public awareness and education so that appropriate risk mitigation measures are not formally applied. In the development and creation of artificial intelligence systems, emphasis must be placed on the possibilities of being able to exercise substantial human supervision over it.

The amounts of data used by artificial intelligence must be of high quality and, following their purpose, relevant, characteristic, free from significant errors and complete. To avoid discrimination, the data set must consider the different information fields relevant to their interpretation. If the data does not meet these requirements, it cannot be ruled out that even a compliant artificial intelligence system will make correct decisions. The extent to which information is collected and the lawfulness of the processing, and the factual veracity of the databases must be ensured throughout.

Low-risk artificial intelligence systems are excluded from the scope of the proposed regulation. However, it is recommended that such systems also comply with mandatory requirements for high-risk systems. It requires analysis of the effects or risks that such systems may entail and the necessary measures to be taken. As the definition of high-risk artificial intelligence systems

in the proposed regulation is open, it cannot be ruled out that an initially low-risk system may fall into a high-risk category in the future. In addition, it must be borne in mind that any voluntary introduction of measures will undoubtedly help increase credibility, which will positively affect the sector as a whole.

The author considers that the proposed regulation, in conjunction with the relevant rules of the GDPR, is sufficient to ensure the transparency of artificial intelligence systems, even in cases where there is no human intervention in the system's decision-making process. However, the compliance of artificial systems with the established requirements must be ensured, and particular emphasis must be placed on upgrading already established procedures and raising public awareness. To achieve adequate transparency, preventive action is the key to understanding even more complex systems in the future. Understanding the processes must complement other requirements so that artificial intelligence systems do not become vulnerable to possible attacks or errors that can accumulate over time.

Like the European Union legislation, Estonia plans to develop a law on artificial intelligence systems, which is to regulate artificial intelligence systems as a whole. In terms of its content and starting point, it is strongly related to the proposed regulation and provides an opportunity to specify the regulation if necessary. In particular, the intention to draft a law emphasizes the importance of communication, through which it is possible to mitigate the risks arising from artificial intelligence. In light of the proposed Regulation of the European Parliament and of the Council, it is still necessary to determine the extent to which further regulation of artificial intelligence systems in Estonian law is required. It is more important to explain what form and for what purposes it is reasonable to use the respective systems at the national level.

The effects of the proposed regulation are broad, leading to a more significant opportunity to implement and use artificial intelligence systems. Public and private bodies that already use artificial intelligence systems will gain more assurance that their activities meet the applicable requirements. However, in the initial phase of the regulation coming into force, it must be borne in mind that bringing existing systems into line with the requirements will increase the workload. Still, it will not have a disproportionately negative impact on procedures in the case of targeted action. By implementing automated systems, public authorities can increasingly

focus on issues requiring more substantive analysis, which will help make processes more efficient and reduce administrative burden.

The analysis of the master's thesis revealed that the use of artificial intelligence in compiling profile analysis or making other automated individual decisions poses a significant risk to the fundamental rights and freedoms of natural persons. To address artificial intelligence opacity, several requirements need to be put in place to mitigate the risks. Transparency of the process can be achieved based on the specific requirements that the proposed regulation imposes on artificial intelligence systems. These requirements, together with other measures, will ensure sufficient transparency of artificial intelligence systems. Still, it must be borne in mind that compliance must be effectively monitored, and awareness raised in this area. All this requires a broad-based and comprehensive approach. It must be acknowledged that, given the freshness of the regulation, the problem statement requires even closer analysis if the bottlenecks and possible difficulties related to its implementation become clear.

LÜHENDID

DARPA – Defense Advanced Research Projects Agency

GDPR – General Data Protection Regulation

IKS – Isikuandmete kaitse seadus

IKÜM – Euroopa Liidu isikuandmete kaitse üldmäärus

Krati VTK – Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus

RahaPTS – Rahapesu ja terrorismi rahastamise tõkestamise seadus

xAI – Explainable Artificial Intelligence

KASUTATUD ALLIKAD

RAAMATUD, ARTIKLID JA TEADUSTÖÖD

1. Barocas, S. Selbst, A. D. Big Data's Disparate Impact. – California Law Review 2016/104, No. 3. – https://www.jstor.org/stable/24758720 (12.04.2021).
2. Baum, S. Barrett, A. Yampolskiy, R. Modelling and Interpreting Expert Disagreement About Artificial Superintelligence. – Informatica 2017/41, No. 7. – https://ssrn.com/abstract=3104645 (08.03.2021).
3. Begishev, I. Latypova E. Kirpichnikov, D. Artificial Intelligence as a Legal Category: Doctrinal Approach to Formulating a Definition. – Actual Problems of Economics and Law 2020/1. – https://heinonline.org/HOL/Page?public=true&handle=hein.journals/apel2020&div=8&start_page=79&collection=journals&set_as_cursor=0&men_tab=srchresults (24.02.2021).
4. Bengio Y, Goodfellow I, Courville A. Deep learning. Massachusetts: MIT press 2017.
5. Buttarelli, G. Assessing the Necessity of Measures that Limit the Fundamental Right to the Protection of Personal Data: a Toolkit. Brussels: European Data Protection Supervisor 2017. – https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf (03.04.2021).
6. Chen, X.W. Lin, X. Big Data Deep Learning: Challenges and Perspectives. – IEEE Access 2014/2. – https://ieeexplore.ieee.org/abstract/document/6817512 (16.03.2021).
7. Coglianese, C. Lehr, D. Regulating by Robot: Administrative Decision Making in the Machine-Learning Era. – The Georgetown Law Journal 2017/105, No. 5. – https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=2736&context=faculty_scholarship (07.04.2021).
8. De Hert, P. Gutwirth, S. Privacy, data protection and law enforcement. Opacity of the individual and transparency of power. Privacy and the Criminal Law. Antwerpen-Oxford: Intersentia 2006.
9. Deeks, A. The judicial demand for explainable artificial intelligence. – Columbia Law Review 2019/119, No. 7. – https://www.jstor.org/stable/26810851 (19.04.2021).
10. Eneken, T. Nõmper, A. Informatsioon ja õigus. Tallinn: Juura 2007.

11. European Union Agency for Fundamental Rights and Council of Europe. Handbook on European data protection law. Luxembourg: Publications Office of the European Union, 2018. – https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (11.04.2021).
12. Felzmann, H. Villaronga, E. F. Lutz, C. Tamo-Larrieux, A. Transparency you can trust: Transparency requirements for artificial intelligence between legal norms and contextual concerns. – Big Data & Society 2019. – https://journals.sagepub.com/doi/pdf/10.1177/2053951719860542 (10.04.2021).
13. Goertzel, B. Artificial general intelligence (Vol.2). Edited by Pennachin C. New York: Springer 2007.
14. Grimmelikhuijsen, S. Porumbescu, G. Hong, B. Im, T. The effect of transparency on trust in government: A cross-national comparative experiment. – Public Administration review 2013/73, No. 4. – https://doi.org/10.1111/puar.12047 (05.04.2021).
15. Gunning, D. Aha, D. DARPA's Explainable Artificial Intelligence (XAI) Program. – AI Magazine 2019/40, No.2. – https://doi.org/10.1609/aimag.v40i2.2850 (14.04.2021).
16. Haney, B. S. The perils and promises of artificial general intelligence. – Journal of Legislation 2018/45, No. 2. – https://heinonline.org/HOL/Page?handle=hein.journals/jleg45&div=10&g_sent=1&casa_token=&collection=journals (28.02.2021).
17. Humerick, M. Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence. – Santa Clara High Technology Law Journal 2018/34, No. 4. – https://heinonline.org/HOL/LandingPage?handle=hein.journals/sccj34&div=19&id=&page= (09.03.2021).
18. Kaplan, A. Haenlein, M. Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. – Business Horizons 2019/62, No. 1. – https://www.sciencedirect.com/science/article/pii/S0007681318301393 (28.02.2021).
19. Karageorgu, V. Transparency principle as an evolving principle of EU law: Regulative contours and implications. – https://www.right2info.org/resources/publications/eu-karageorgou-vasiliki-transparency-principle-as-an-evolving-principle-of-eu-law/view (10.04.2021).
20. Koit, M. Roosma, T. Tehisintellekt. Tartu Ülikooli arvutiteaduse instituut. Tartu: Tartu Ülikooli kirjastus 2011. -

https://dspace.ut.ee/bitstream/handle/10062/28296/tehisintellekt.pdf?sequence=2&isAllowed=y (27.02.2021).

21. Kroll, J. A. Huey, J. Barocas, S. Felten, E. W. Reidenberg, J. R. Robinson, D. G. Yu, H. Accountable Algorithms. – University of Pennsylvania Law Review 2017/165, No.3. – https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9570&context=penn_law_review (12.04.2021).
22. Kruuse, K. Privaatsuse ja isikuandmete kaitse masinnägemise ja masinõppe kasutusel Euroopa Liidu õiguses emotsioonituvastuse ja Eesti korrakaitse jälgimisseadmestike näitel. Tallinn 2019. - https://dspace.ut.ee/handle/10062/64059 (02.04.2021).
23. Langemets, M. jt. Eesti keele seletav sõnaraamat. „Eesti kirjakeele seletussõnaraamatu" 2., täiendatud ja parandatud trükk. Tallinn: Eesti Keele Sihtasutus 2009. – https://www.eki.ee/dict/ekss/index.cgi?Q=tehisintellekt&F=M (27.02.2021).
24. Lember, K. Tehisintellekti kasutamine haldusakti andmisel. Tartu 2019. – https://dspace.ut.ee/handle/10062/64057 (02.04.2021).
25. Lepri, B. Oliver, N. Letouzé, E. Pentland, A. Vinck, P. Fair, Transparent, and Accountable Algorithmic Decision-making Processes. – Philosophy & Technology 2018/31, No. 4. – https://link.springer.com/article/10.1007/s13347-017-0279-x#citeas (04.04.2021).
26. Mohri, M. Rostamizadeh, A. Talwalkar A. Foundations of machine learning. Cambridge: The MIT Press 2018.
27. Ng, G.W. Leung, W.C. Strong Artificial Intelligence and Consciousness. – Journal of Artificial Intelligence and Consciousness 2020/7, No. 1. – https://www.worldscientific.com/doi/epdf/10.1142/S2705078520300042 (08.03.2021).
28. Pilving, I. Mikiver, M. Kratt haldusorganiks: algoritmilised otsused ja haldusõiguse põhimõtted. – Kohtute aastaraamat 2019. Tartu: Riigikohus 2019. – https://aastaraamat.riigikohus.ee/kratt-haldusorganiks-algoritmilised-otsused-ja-haldusoiguse-pohimotted/#_ftn33 (05.04.2021).
29. Politou, E. Alepis, E. Patsakis, C. Profiling tax and financial behaviour with big data under the GDPR. – Computer Law & Security Review 2019/35, No. 3. – https://doi.org/10.1016/j.clsr.2019.01.003 (18.04.2021).
30. Robinson, S. C. Trust, transparency, and openness: How inclusion of cultural values shapes Nordic national public policy strategies for artificial intelligence (AI). –

Technology in Society 2020/63. – https://doi.org/10.1016/j.techsoc.2020.101421 (05.04.2021).

31. Rücker, D. Kugler, T. New European General Data Protection Regulation. A Practitioner's Guide. Baden-Baden: Nomos Verlagsgesellschaft 2018.
32. Russell, J.S. Norvig, P. Artificial Intelligence. A Modern Approach. Third Edition. New Jersey: Pearson 2010.
33. Sartor, G. Lagioia, F. The impact of the General Data Protection Regulation (GDPR) on artifical intelligence. Brussels: European Parliamentary Research Service 2020. – https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf (10.04.2021).
34. Schermer, B. W. The limits of privacy in automated profiling and data mining. – Computer Law & Security Review 2011/27, No.1. – https://doi.org/10.1016/j.clsr.2010.11.009 (18.04.2021).
35. Stoyanovich, J. Goodman, E. P. Revealing Algorithmic Rankers. – Freedom to Tinker 2016. – https://freedom-to-tinker.com/2016/08/05/revealing-algorithmic-rankers/ (27.04.2021).
36. Surden, H. Artificial Intelligence and Law: An Overview. – Georgia State University Law Review 2019/35. – https://ssrn.com/abstract=3411869 (09.03.2021).
37. Temme, M. Algorithms and Transparency in View of the New General Data Protection Regulation. – European Data Protection Law Review (EDPL) 2017/3, No. 4.
38. Tizhoosh, H.R. Pantanowitz, L. Artificial intelligence and digital pathology: Challenges and opportunities. – Journal of pathology informatic 2018/9. – http://www.jpathinformatics.org/text.asp?2018/9/1/38/245402 (28.02.2021).
39. Tzanou, M. The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance. Oxford-Portland: Hart Publishing 2017.
40. Van Engelen, J.E. Hoos, H.H. A survey on semi-supervised learning. – Machine Learning 2020/109, No.2. – https://doi.org/10.1007/s10994-019-05855-6 (11.03.2021).
41. Van Nuenen, T. Ferrer, T. X. Such, J. M. Cote, M. Transparency for Whom? Assessing Discriminatory Artificial Intelligence. – Computer 2020/53, No. 11. – https://ieeexplore.ieee.org/abstract/document/9237325 (27.04.2021).
42. Voigt, P. Von dem Bussche, A. The EU General Data Protection Regulation (GDPR). A Practical Guide. Cham: Springer International Publishing 2017.

43. Weller, A. Transparency: motivations and challenges. In Explainable AI: Interpreting, Explaining and Visualizing Deep Learning. Cham: Springer 2019. – https://link.springer.com/chapter/10.1007/978-3-030-28954-6_2 (27.04.2021).
44. Žuk, J. Ärisaladuse ja isikuandmete kaitse regulatsiooni interaktsioon tehisintellekti läbipaistvuse tagamisel. Tallinn 2019. - http://dspace.ut.ee/handle/10062/64755 (02.04.2021).

ÕIGUSAKTID

1. 24.oktoobri 1995.aasta Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, lk 0031 – 0050.
2. 27. aprilli 2016. aasta Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, millega kehtestatakse füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, lk 1—88.
3. Euroopa Liidu põhiõiguste harta. – ELT C 326/391, 26.10.2012, lk 391 – 407.
4. Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.
5. Rahapesu ja terrorismi rahastamise tõkestamise seadus. – RT I, 17.11.2017, 2.

KOHTUPRAKTIKA

1. EK C-101/01, *Bodil Lindqvist*, ECLI:EU:C:2003:596.
2. EK C-110/03, *Belgia Kuningriik* versus *komisjon,* ECLI:EU:C:2005:223, kohtujurist D. Ruiz-Jarabo Colomer ettepanek.
3. EK C-582/14, *Patrick Breyer versus Saksamaa Liitvabariik*, ECLI:EU:C:2016:779.

MUUD ALLIKAD

1. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe, COM/2018/237 final. Brussels,

25.04.2018. – https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN (27.02.2021).

2. Euroopa Komisjon. Valge Raamat. Tehisintellekt: Euroopa käsitus tipptasemel ja usaldusväärsest tehnoloogiast, COM/2020/65 final. Brüssel, 19.02.2020. – https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_et.pdf (27.03.2021).
3. Justiitsministeerium. Algoritmiliste süsteemide mõjude reguleerimise väljatöötamise kavatsus. 14.08.2020. – https://adr.rik.ee/jm/dokument/7458502 (19.04.2021).
4. Majandus- ja Kommunikatsiooniministeerium. Eesti riiklik tehisintellekti alane tegevuskava 2019-2021. – https://www.mkm.ee/sites/default/files/eesti_kratikava_juuli2019.pdf (19.04.2021).
5. Riigikantselei ja Majandus- ja Kommunikatsiooniministeerium. Eesti tehisintellekti kasutuselevõtu eksperdirühma aruanne. Mai 2019. Avalikult kättesaadav krattide projekti kodulehel: https://www.kratid.ee/ (19.04.2021).
6. Swedbank AS Kliendiandmete töötlemise põhimõtted. – https://www.swedbank.ee/static/pdf/private/home/important/gdpr/Principles_of_processing_Personal_data_EE_EST_01032021.pdf (01.03.2021).
7. The Article 29 Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251. – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (20.04.2021).
8. The Article 29 Working Party. Guidelines on Transparency under Regulation 2016/679, WP260. – https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227&fbclid=IwAR08HU1Akd29jRoWMzlFJq2cOQZ1_Rz6ldclrKmI9TAE-ah5809C7er1Bjw (21.04.2021).
9. The Council of Europe. Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Council of Europe Treaty Series - No. 223. Strasbourg, 2018. – https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a (21.04.2021).
10. The Defence Agency Research Projects Agency. Broad Agency Announcement on Explainable Artificial Intelligence (XAI). Arlington, 10.08.2016. – https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf (19.04.2021).

11. The European Commission. ANNEXES to the Proposal for a Regulation of the European Parliament and of the Council, COM/2021/206 final. Brussels, 21.04.2021. – https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence-artificial-intelligence (27.04.2021).
12. The European Commission. Proposal for a Regulation on a European approach for Artificial Intelligence, COM/2021/206 final. Brussels, 21.04.2021. – https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence (24.04.2021).
13. The European Commission`s High-Level Expert Group on Artificial Intelligence. A definition of AI: Main capabilities and scientific disciplines. Brussels, 08.04.2019. – https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines (11.03.2021).
14. The European Commission's High-Level Expert Group on Artificial Intelligence. Ethics Guidelines for Trustworthy AI. Brussels, 08.04.2019. – https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (05.04.2021).