TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Eraõiguse osakond

Jana Žuk

ÄRISALADUSE JA ISIKUANDMETE KAITSE REGULATSIOONI INTERAKTSIOON TEHISINTELLEKTI LÄBIPAISTVUSE TAGAMISEL

Magistritöö

Juhendaja:

Prof. Aleksei Kelli

Tallinn

2019

SISUKORD

SISSEJUHATUS

Tänapäeval areneb tehnika hüppelise kiirusega ning üha enam sõltuvad inimesed igapäevaelus nutikatest tehnoloogilistest vahenditest. Paljud tehnoloogilised lahendused, mida oleme harjunud nägema ulmefilmides, ei kuulu aga enam ainult ulmevaldkonda, vaid on saanud reaalsuseks. Suurimaks 21.sajandi arenguhüppeks on olnud tehisintellekti kasutuselevõtt paljudes eluvaldkondades. Tehisintellektid on leitavad nutitelefonides, tahvel-, sülearvutites ja muudes seadeldistes, tuvastades ja parandades meie õigekirja, aidates meil hääljuhtimise abil saada küsimustele vastused, soovitades kirjandusteoseid ja muusikapalasid.[1] Autonoomsed sõidukid[2] ja relvad ei ole samuti kauge tuleviku temaatika, vaid need on käesoleval ajal juba kasutuses. Masinad suudavad luua kunsti, komponeerida muusikat, määrata meditsiinilisi diagnoose, analüüsida juriidilisi materjale ja palju muudki.[3] Kahjuks aga intelligentsed masinad toovad endaga kaasa palju riske, mistõttu tehisintellekt on osutunud aktuaalseks nii rahvusvahelisel kui riigisisestel tasanditel eetikakoodeksi ja seadusandluse väljatöötamise võtmes.

2018. aasta märtsikuus käivitasid Eesti Riigikantselei ning Majandus- ja Kommunikatsiooniministeerium valdkonnaülese projekti tehisintellekti ehk krattide kasutuselevõtmise analüüsimiseks ja ettevalmistamiseks Eestis. Ekspertrühma ülesandeks on koostada seaduseelnõu, muutmaks võimalikuks krattide kui täisautonoomsete infosüsteemide kasutamine kõikvõimalikes eluvaldkondades ning samaaegselt tagamaks õigusruumi selgus ja vajalik järelevalve. Samuti töötab ekspertrühm välja Eesti tehisintellekti strateegia, millistest krattidest võib enim kasu olla nii avalikus kui erasektoris ning meetmed, millega nende kasutuselevõtmist edendada. Ekspertrühm esitab väljatöötatud strateegia ja seaduseelnõu

[1] Apple Siri – hääljuhtimisel baseeruv isiklik assistent telefonis, vt https://www.apple.com/ios/siri/, Samsung Bixby – taskuassistent, https://www.androidcentral.com/bixby (01.03.2019)

[2] R. Kinkar. Tootjavastutus ja juhi deliktiõiguslik vastutus autonoomsete sõidukite tehnoloogia puudusest tingitud kahju tekkimise korral. Tartu: TÜ Õigusteaduskond 2015. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/46852/kinkar_rauno.pdf (01.02.2019)

[3] AI Composer Creates Music for Films and Games. – NVIDIA Developer, 16.03.2017. Arvutivõrgus: https://news.developer.nvidia.com/ai-composer-creates-music-for-films-and-games/; C. Quackenbush, A Painting Made by Artificial Intelligence Has Been Sold at Auction for $432,500. 26.10.2018. TIME USA, LLC. Arvutivõrgus: http://time.com/5435683/artificial-intelligence-painting-christies/ (01.02.2019); Sorainen. Sorainen võttis kasutusele Luminance'i tehisintellekti tehnoloogia. 25.10.2018. Arvutivõrgus: https://www.sorainen.com/et/sorainen-vottis-kasutusele-luminancei-tehisintellekti-tehnoloogia/ (01.02.2019)

aprillis 2019.[4] Euroopa Liidu tasandil allkirjastasid liikmesriigid 10. aprillil 2018. aastal koostöö deklaratsiooni tehisintellekti valdkonnas. Liikmesriigid leppisid kokku, et teevad koostööd kõige tähtsamate küsimuste lahendamisel, alates konkurentsivõime tagamisest tehisintellekti uurimisel ja lõpetades sotsiaalsete, majanduslike, eetiliste ja õiguslike küsimustega.[5]

Tänapäeval on raske üheselt defineerida tehisintellekti olemust, kuivõrd definitsioonid põhinevad peamiselt tehisintellektile püstitatud ülesande ja selle lahenduse olemusest.[6] Tehisintellekti on Eesti keele sõnaraamatus defineeritud esmalt kui modelleeritud ajuprotsessidest tulenevat arvuti suutlikkust jäljendada inimese vaimset tegevust ehk tehisaruna, ning teisalt kui arvutiteaduse ja -tehnika haruna, mis uurib ajuprotsesside modelleerimist elektronarvutil ja vastavate arvutisüsteemide loomise meetodeid.[7] Teisisõnu tehisintellekt jäljendab loomulikku intellekti, mis tähendab arvutisüsteemi võimet täita funktsioone, mida üldiselt seostatakse inimmõistusega, sealhulgas arutlemine ja õppimine.[8] Täpsemalt on tegemist infotehnoloogilise süsteemiga, mis baseerub iseõppivatel algoritmidel.[9] Tehisintellekti eesmärgiks on lahendada keerulised ülesanded kas füüsilises või digitaalses keskkonnas, töödeldes ja tõlgendades kogutud andmehulkasid ning otsustada talle püstitatud ülesande lahendamisel parima võimaliku toimingu kasuks. Ühtlasi suudab tehisintellekt analüüsida, kuidas tema käitumine mõjutab ümbritsevat keskkonda.[10] Tegemist on äärmiselt

---

[4] Riigikantselei. Eesti saab tehisintellekti strateegia. 27.03.2018. Arvutivõrgus: https://www.riigikantselei.ee/et/uudised/eesti-saab-tehisintellekti-strateegia (01.02.2019)

[5] Euroopa Komisjon. EU Member States sign up to cooperate on Artificial Intelligence. 10.04.2018. Arvutivõrgus: https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence (02.02.2019)

[6] B. Marr. The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance. 14.02.2018. Arvutivõrgus: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/ (02.02.2019)

[7] M. Langemets jt (toim.). Eesti keele seletav sõnaraamat. „Tehisintellekt". Eesti Keele Sihtasutus 2009. Arvutivõrgus: http://www.eki.ee/dict/ekss/index.cgi?Q=tehisintellekt&F=M (02.02.2019)

[8] M. Koit, T. Roosmaa. Tehisintellekt. Tartu: TÜ Arvutiteaduse instituut 2011. Arvutivõrgus: https://dspace.ut.ee/bitstream/handle/10062/28296/tehisintellekt.pdf?seq (02.02.2019)

[9] M. Aim. Tehisintellekti kasutamispraktikad ja arenguperspektiivid Eesti finantssektori näitel. Tartu: TÜ Majandusteaduskond 2018. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/61160/aim_mariel.pdf?sequence=1&isAllowed=y (02.02.2019)

[10] The European Commission's high-level expert group on artificial intelligence. A definition of AI: main capabilities and scientific disciplines. Definition developed for the purpose of the deliverables of the High-Level

keerulise valdkonnaga, kuivõrd algoritmid käituvad kui „must kast“ – isegi selle loonud inimene ei oska alati öelda, miks algoritm just sellise otsuse vastu võttis. Tehisintellekti otsustusel ei ole alati klassikalist põhjus-tagajärg seost, nagu ollakse harjunud kohtama senistes tarkvarades, küll aga on võimalik algoritme treenida paremaks ja tõhusamaks. [11]

Viimaste aastate tehnoloogia arengu, selle võimekuse ja tehisintellekti kasutusele võtmisega on suurenenud andmete sissevoolavus ja maht. Ettevõtted koguvad ja töötlevad suurandmeid (inglise keeles *Big Data*) struktureeritud ja struktureerimata vormidena lõputult. Paraku on suurandmete haldamise probleemkohaks ekspertide puudus, kes suurandmete sisu mõistaksid ja praktiliselt rakendada oskaksid, seetõttu on andmetöötluse protsessi lihtsustamiseks kasutusele võetud just tehisintellektil põhinevaid tarkvaralahendusi, mis suudavad kõiki andmehulkasid läbi töötada ja mõista. Kuivõrd algoritmid arenevad, suureneb nende mõju ka andmehaldusele. Masinõpe on andmetepõhine prognoosimis- ja otsustamisalgoritm, mis kombineeritult naturaalse keele töötlemisega, suudab vastupidiselt üksikisikule esitada kasulikku teavet ja lahendusi äristrateegiate kohta üldise eesmärgiga suurendada tootlikkust ja konkurentsivõimet turul.[12]

Suuremahuline andmetöötlus tehisintellektide kasutus perspektiivis ohustab inimeste põhiõigusi, eelkõige õigust privaatsusele. Sellest tulenevalt peab rahvusvahelisel ja riigisisesel tasandil reguleerima turvalise andmetöötluse tagamise meetmeid ning kavandama regulatsioon, mis oleks vastavuses tehnika kiire arenguga, takistamata sealjuures innovatsiooni levikut. Inimeste turvalisuse tagamiseks on Euroopa Parlament ja Nõukogu võtnud vastu määruse 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta (edaspidi kasutatakse mõistet üldmäärus või lühendit GDPR), mida kohaldatakse alates 25. maist 2018.[13] Isikuandmete kaitse üldmäärus toob esile mitmeid põhimõtteid, millest üks olulisemaid andmete töötlemisel on läbipaistvuse põhimõte.

Expert Group on AI. Brüssel, 18.12.2018. Arvutivõrgus: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december.pdf (02.02.2019)

[11] Riigikantselei (viide 4)

[12] CLEVERISM. Artificial Intelligence: A Complete Guide. 2015. Arvutivõrgus: https://www.cleverism.com/artificial-intelligence-completeguide/ (02.02.2019)

[13] Euroopa Parlamendi ja Nõukogu määrus 2016/679, 27. aprill 2016, 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, 04.05.2016 (edaspidi viidatud ka GDPR)

Üldmääruse põhjendus nr 39 ütleb, et läbipaistvuse põhimõte eeldab isikuandmete töötlemisega seotud teabe ja sõnumite lihtsat kättesaadavust, arusaadavust ning selget ja lihtsat sõnastust. Üldsusele või andmesubjektile suunatud teave peab olema kokkuvõtlik, kergelt sõnastatud ning vajaduse korral tuleks täiendavalt kasutada visualiseerimist (üldmääruse põhjendus nr 58). Tehisintellekti arendavate ja loovate ettevõtete jaoks tähendab andmetöötluse läbipaistvuse tagamine asjaolu, et iseõppivaid algoritme tuleb tavakodanike jaoks võimalikult lihtsas keeles ja arusaadavalt selgitada. Algoritmide selgitamine andmetöötluse läbipaistvuse tagamisel võib tekitada olukorra, kus ettevõtted on regulatsiooni täitmiseks sunnitud avaldama enda ärisaladuse ja seadma ohtu enda konkurentsivõimelisuse.

Eeltoodust tulenevalt analüüsib käesolev magistritöö tehisintellekti kui „musta kasti" kontseptsiooni, Euroopa Liidu ja Eesti riigisisese õiguse tasandil kehtivaid regulatsioone andmetöötluse ja intellektuaalse omandi kohta iseõppivate algoritmide kontekstis. Töö kirjutamise käigus uurib autor põhjalikult üldmäärusest tulenevat läbipaistvuse põhimõtet ja paralleelselt Eesti riigisisest õigust, analüüsimaks, kuidas seadusandjad on põhimõtet sisustanud ja selle kohaldamist ette näinud olukorras, kus tehisintellekti loojatel või asjatundjatel puudub täielik ülevaade iseõppivate algoritmide käitumisest. Analüüsi käigus selgub, kas füüsilise isiku asjakohased põhiõigused (nagu õigus privaatsusele ja informatsioonile) on kaitstud ja tähtsustatud suuremal määral kui ettevõtjate põhiõigus ettevõtlusele ja konkurentsivõimelisusele ärisaladuse kaitstuse kontekstis. Seega käesoleva töö eesmärgiks on välja selgitada, kas isikuandmete töötlemisel on võimalik tagada täielikku läbipaistvust ja selgust tehisintellekti algoritmide iseõppimise käigus tehtavatele otsustustele. Autor analüüsib tehisintellektil põhinevatel tarkvaralahenduste ärisaladuse kaitset ja seeläbi konkurentsivõimekuse tagamist ilma füüsiliste isikute privaatsuse rikkumiseta andmetöötluse perspektiivis. Samuti teeb autor ettepanekuid Eesti riigisisese regulatsiooni täiendamiseks või muutmiseks tehisintellekti andmekaitse ja ärisaladuse problemaatikat sidudes.

Eesmärkideni jõudmiseks seab autor hüpoteesi, et isikuandmete kaitse regulatsioon piirab eraõiguslike juriidiliste isikute põhivabadust tegeleda ettevõtlusega ja läbipaistvuse tagamine ärisaladuse konfidentsiaalsusnõude aspektis takistab konkurentsvõimekust, mistõttu täielikku läbipaistvust isikuandmete töötlemisel ei ole võimalik saavutada. Analüüsi tulemusena peaksid saama vastused alljärgnevad küsimused:

1. Kuidas on Euroopa Liit sisustanud läbipaistvuse nõuet andmete töötlemisel tehisintellektisüsteemide perspektiivis?

2. Kas tehisintellekti iseõppivad algoritmid kuuluvad ärisaladuse kaitse alla ning kas algoritmide avaldamine võib mõjutada konkurentsi?
3. Kas õiguslikult tuleks ettevõtteid kohustada tehisintellekti algoritmi läbipaistvaks tegemiseks?

Magistritöö eesmärkide saavutamiseks ja hüpoteesi kinnitamiseks või tagasilükkamiseks on käesolev töö jaotatud mitmeks peatükiks. Esimeses peatükis analüüsib autor tehisintellekti kui iseõppivat algoritmi, suurandmeid ja nende omavahelist seost. Teises peatükis määratleb autor tehisintellektile kohase õigusraamistiku Euroopa Liidu ja Eesti seadusandluse tasandil ja analüüsib andmetöötluses isikute kaitseks kehtestatud läbipaistvuse põhimõtet, hinnates läbipaistvuse tagamise kohustuse ulatust eraõiguslikele juriidilistele isikutele. Kolmandas peatükis on analüüsiobjektiks konkurentsiõiguse ja ärisaladuse kaitse regulatsioonid, mis on asjakohased iseõppivate algoritmide vaates, aidates käesoleva töö autoril vastata ülaltoodud uurimisküsimustele. Temaatika aktuaalsus seisneb peamiselt isikuandmete ja ärisaladuse kaitse regulatsioonide vastuolus, milles ühelt poolt on ettevõtjad kaitstud omandipõhiõiguse ja ettevõtlusvabadusega ning teiselt poolt füüsilistel isikutel on õigus privaatsusele ja informatsioonile. Enda hinnangu eesmärgi saavutamise ja hüpoteesi kinnitamise või tagasilükkamise kohta annab autor töö kokkuvõttes.

Magistritöö kirjutamisel on aluseks võetud analüütiline uurimismeetod. Kasutusel on ka süsteemne-kvalitatiivne meetod, kuivõrd autor arutleb hüpoteesis seonduva problemaatika ja kehtiva õiguse vajalike kohanduste üle ning teeb vastavaid ettepanekuid. Probleemi uurib autor mitteempiiriliste meetoditega, mistõttu on tegu teoreetilise uurimusega. Magistritöö tugineb Euroopa Liidu asjakohastele õigusaktidele, millest peamise tähtsusega käesolevas töös on Euroopa Parlamendi ja Nõukogu määrus 2016/679 ja Euroopa Parlamendi ja Nõukogu direktiiv 2016/943 (ärisaladuse kaitse direktiiv), ning Eesti riigisisestele õigusaktidele, mis on kehtestatud lähtuvalt Euroopa Liidu õigusest. Tulenevalt tehisintellekti ja isikuandmete kaitse temaatika aktuaalsuse kasvust ja valdkonna jätkuvast arengust, kasutatakse töös peamiselt erialakirjandust, teadustöid ja –artikleid. Läbipaistvuse küsimuses iseõppivate algoritmide suhtes kohtulahendite vähesusest hoolimata, kasutab käesoleva töö autor ka Eesti kohtupraktikat peamiselt ärisaladuse temaatika juures.

1. TEHISINTELLEKT

1.1. Tehisintellekti mõiste, olemus ja masinõpe

Esimene tehisintellekti definitsioon pärineb 1950. aastast, mil inglise matemaatik A. M. Turing pani aluse „imitatsioonimängule"[14], teisisõnu Turingi testile. Testi eesmärk on anda vastus küsimusele, kas masin on võimeline mõtlema, esitades masinale loomulikus keeles küsimusi ning masin püüab kujutada inimest läbi kirjavahetuse, vastates talle esitatud küsimustele. Testi läbimise eelduseks pole kõikidele küsimustele õigesti vastamine, kuivõrd inimene pole samuti eksimatu, vaid masina suutlikus imiteerida inimese poolt antavaid vastuseid nii, et pole võimalik teha vahet, kes küsimustele vastajaks on – kas masin või reaalne isik.[15] Masin peab testi läbimiseks olema võimeline töötlema loomulikku inimkeelt ja suuteline edukalt kommunikeeruma; esitama ja hoiustama enda teadmisi; omama automatiseeritud kaalutlusvõimet kogutud informatsiooni kasutades küsimustele vastamiseks ja uute järelduste tegemiseks; kogutud teadmiste põhjal õppida kohanema uutes oludes ning leidma mustreid.[16]

Tehisintellekti termin (*artificial intelligence)* võeti esmakordselt kasutusele 1956. aastal, kui arvutiteadlane John McCarthy kutsus kokku erinevate valdkondade teadlaste grupi, kelle ühiseks eesmärgiks oli jäljendada arvutil inimese intellekti, püüdes panna arvutit kasutama inimkeelt, moodustama abstrakte ja kontseptsioone, lahendama inimestele antud ülesandeid ning arendama iseend.[17] 1990. aastal pandi dr Hugh Loebneri algatusel välja kuldmedal ja 100 000 USA dollari suurune auhind arvutiprogrammi eest, mis suudab esimesena läbida Turingi testi. Sellest ajast alates korraldatakse iga-aastaseid võistluseid, kus eksperdid hindavad inglise keeles suhtlevaid arvutiprogramme. Hoolimata asjaolust, et tehnoloogia areng on olnud hüppeline ja kiire, pole tänase päevani ükski arvutiprogramm suutnud toime tulla Turingi testi läbimisega – Loebneri auhinda on välja antud vaid pronksmedalite ja lohutusauhindadena.[18]

---

[14] A. M. Turing. Computing Machinery and Intelligence. - Mind 49, 1950. Arvutivõrgus: https://www.csee.umbc.edu/courses/471/papers/turing.pdf (02.02.2019)

[15] M. Koit, T. Roosmaa (viide 8), lk 7

[16] S. J. Russell, P. Norvig. Artificial Intelligence: A Modern Approach. Third Edition. New Jersey: Pearson Education Inc. 2010. Arvutivõrgus: http://aima.cs.berkeley.edu/ (02.02.2019), lk 2

[17] *Ibid*, lk 17

[18] AISB. The Society for the Study of the Artificial Intelligence and Simulation of Behaviour. Loebner Prize. Arvutivõrgus: https://www.aisb.org.uk/events/loebner-prize (02.02.2019)

Eesti keele seletav sõnaraamat ja võõrkeelsete sõnade leksikon defineerivad tehisintellekti esiteks kui modelleeritud ajuprotsessidest tulenevat arvuti suutlikkust jäljendada inimese vaimset tegevust (tehisaru) ning teiseks kui arvutiteaduse ja -tehnika haru, mis uurib ajuprotsesside modelleerimist elektronarvutil ja vastavate arvutisüsteemide loomise meetodeid.[19] Mõistet tehisintellekt kasutatakse seega kahes tähenduses – tehisintellekt võib tähistada nii teatava arvutisüsteemi omadust käituda sarnaselt inimesele kui ka uurimissuunda, mis tegeleb selliste arvutisüsteemide kui tehisintellektisüsteemide väljatöötamisega. Uurimissuuna tähistamiseks kasutatakse eesti keeles ka terminit intellektitehnika.[20] IT terministandardi sõnastik lisab, et tegemist on informaatika haruga, mis tegeleb selliste andmetöötlussüsteemide arendamisega, mis täidavad inimmõistusele omaseid funktsioone nagu arutlemine, õppimine ja enesetäiendus.[21]

Tehisintellekt on arvutiteaduse haru ja tehnoloogia, mille eesmärk on suunatud selliste teooriate, meetodite, rakenduste ja algoritmide arendamisele, mis jäljendavad ja laiendavad inimintelligentsust. Kui vana maailma intellekt sai inimestelt konkreetsed reeglid probleemide lahendamiseks, võimaldab kaasaaegne tehisintellekt minna üle uuele maailmale, kus inimesed annavad intellektile üle lahendatava probleemi, mille masin õpib ise lahendama, kasutades selleks algoritmide kogumit.[22] Tehisintellekti poolt andmete töötlemine, seosete loomine ja iseõppimine toimubki algoritmide abiga.[23] Algoritm on iseseisev jada juhiste ja toimingutega, mida teostab arvutiseade. Oma esialgses olekus ja sisendis kirjeldavad juhised arvutuslikke samme, mille käivitamisel jätkavad need piiratud arvu hästi määratletud olekute läbimist, luues

---

[19] Tehisintellekt – e-keelenõu. Eesti Keele Instituut. 2013. Arvutivõrgus: http://kn.eki.ee/?Q=tehisintellekt (02.02.2019)

[20] M. Koit, T. Roosmaa (viide 8), lk 6

[21] Tehisintellekt – IT Terministandardi sõnastik. Arvutivõrgus: http://www.keeleveeb.ee/ (02.02.2019). Lisaks tähendab tehisintellekt funktsionaalüksuse võimet täita selliseid funktsioone, mis üldiselt on seostatavad inimmõistusega, nt arutlemine ja õppimine. Kusjuures funktsionaalüksus on Etteantud otstarbe täitmiseks võimeline riistvara-, tarkvara- või nende ühismoodustis, vt http://www.keeleveeb.ee/dict/speciality/itstandard/dict.cgi?word=sv1482

[22] L. Deng. Artificial Intelligence in the Rising Wave of Deep Learning - The historical path and future outlook. IEEE Signal Processing Magazine. 2018, lk 180. Arvutivõrgus: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8253597 (02.02.2019)

[23] Deloitte. AI and You: Perceptions of Artificial Intelligence from the EMEA financial services industry. 2017, lk 4. Arvutivõrgus: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology/deloitte-cn-tech-ai-and-you-en-170801.pdf (02.02.2019)

väljundi ja lõpetavad tegevuse lõpp-faasis. Tehisintellekti algoritmid koosnevad algoritmide kogumist, mille abil tehisintellekt täidab talle määratud ülesanded, eelkõige taju ja tunnetavusega seotud ülesanded, mis hõlmavad olemasolevatest andmetest ja kogemustest õppimist, simuleerides inimeste intelligentsust.[24] Tehisintellekti eesmärk on täita ülesandeid, mis inimeste jaoks on liialt keerulised või mille järjepidev teostamine inimese poolt oleks ebaefektiivne ja aeganõudev.[25]

Euroopa Komisjon esitles Euroopa Parlamendile, Euroopa Ülemkogule, Euroopa Nõukogule 2018. aastal teatise „Tehisintellekt Euroopa huvides", millega määratles tehisintellekti olemust kui intelligentselt käituvat süsteemi, mis analüüsib oma keskkonda ja sooritab teataval määral iseseisvaid toiminguid, saavutamaks konkreetseid eesmärke. Intelligentsed süsteemid võivad olla tarkvarapõhised ja tegutseda virtuaalmaailmas. Näiteks põhinevad tehisintellektil kujutise analüüsimise tarkvara, otsingumootorid, häälele reageerivad virtuaalassistendid, kõne- ja näotuvastussüsteemid. Tehisintellekt võib olla ka paigaldatud riistvarasse, nt kõrgtehnoloogilised robotid, isejuhtivad autod, droonid või tehnika internetirakendused.[26]

Tehisintellekte jaotatakse tugevateks (*strong*) ja nõrkadeks (*weak*): nõrga tehisintellekti all mõistetakse tehisnärvivõrke, geneetilisi algoritme ja evolutsioonilisi meetodeid kasutavat tehisintellekti ning tugeva all loogilistel alustel põhinevat tehisintellekti, kusjuures kumbki lähenemisviis ei ole täiuslik ja parima tulemuse võiks anda nende kombinatsioon.[27] Nõrgaks tehisintellektiks nimetatakse süsteemi, millele on lisatud üks kuni mõni inimmõistuse poolt teostatav kitsas funktsioon - näiteks ümbruskonna tajumine, infohulgast erisuste ja mustrite otsimine (sh näo- ja hääletuvastus) ning mille abil arvuti suudab käituda inimesele kohaselt.[28] Tugev tehisintellekt on süsteem, mis on oma suutlikkuse poolest inimese mõistusega võrdväärne ehk süsteem suudab aru saada erinevatest andmetest, oskab kriteeriumeid ette

[24] L. Deng (viide 22), lk 180

[25] S. J. Russell, P. Norvig (viide 16), lk 1034

[26] Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele: Tehisintellekt Euroopa huvides. Brüssel, 2018. Lk 1. Arvutivõrgus: http://ec.europa.eu/transparency/regdoc/rep/1/2018/ET/COM-2018-237-F1-ET-MAIN-PART-1.PDF (05.02.2019)

[27] M. Koit, T. Roosmaa (viide 8), lk 10

[28] J. Russell, P. Norvig (viide 16), lk 1020

andmata need mõistlikesse gruppidesse jaotada, analüüsida, tulemusi kirjeldada, leida sobivaimad lahendused ja vastused tekkinud probleemidele ja küsimustele.[29]

Tehisintellekti üks levinumaid arendamisviise on masinõpe (*machine learning*), mille käigus õpib arvuti lugema erinevaid andmestikke, kohandudes ette tulnud situatsioonide ja probleemidega ilma võimalike lahenduste eelnevalt süsteemi programmeerimiseta või ilma, et mudel neid probleeme ja ülesandeid varem lahendanud oleks.[30] Masinõpe viitab protsessile, mille käigus arvutisüsteem tuvastab andmestikes mustreid ja seoseid automatiseeritult ning süsteem on võimeline masinõppe abil parendama enda jõudlust uute andmetega kokku puutudes ilma vajaduseta järgida selgesõnaliselt programmeeritud juhiseid.[31]

Masinõpe on tehnoloogia, mis võimaldab arvutitel õppida otse andmete vormis saadud näidetest ja kogemustest. Traditsioonilised programmeerimise lähenemisviisid tuginevad püsikodeeritud reeglitel, mis sätestavad probleemi lahenduskäigu samm-sammult ette. Seevastu masinõppe puhul on ülesande lahendamiseks antud ulatuslik hulk andmeid näidetena, kuidas saavutada lahendus ja mille abil luua mustreid. Seejärel süsteem õpib iseseisvalt saadud andmete põhjal, kuidas kõige paremini saavutada soovitud väljund. Seda võib pidada nõrgaks tehisintellektiks: masinõppimine toetab intelligentseid süsteeme, mis suudavad õppida konkreetset funktsiooni, arvestades konkreetseid andmeid, millest õppida.[32] Masinõpe suudab saavutada kõrgema jõudluse kui inimene. Tehisintellekti andmetest õppimise võimekus suurendab masinõppesüsteemide poolt teostatavate funktsioonide arvu ja keerukust võrreldes traditsiooniliste programmeerimismeetoditega. Masinõpe võimaldab teostada nii komplitseeritud ülesandeid, et soovitud väljundeid ei ole võimalik eelnevalt kindlaks määrata ja prognoosida nii nagu inimeste loodud programmide puhul, mis põhinevad samm-sammulistel protsessidel. Õppimiselement loob ka ise uusi algoritmsüsteeme, mis on kohanemisvõimelised ja jätkavad enda tulemuste täpsuse täiustamist.[33]

---

[29] *Ibid*, lk 1026

[30] M. Aim (viide 9), lk 9

[31] Deloitte (viide 23), lk 4

[32] The Royal Society. Machine Learning: The Power and Promise Of Computers That Learn By Example. lk 19 Arvutivõrgus: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf (10.02.2019)

[33] *Ibid* 31

Tehisintellekti arendamisel on põhiväärtus arvuti õpetamisel näidete abil ja mitte käsitsi kodeeritud algoritmidel, seega olulist rolli omavad kasutatavate andmestike suurus ja nende kvaliteet.[34] Oluline ei ole mitte treeningandmeid arvutil mehaaniliselt „meelde jätta“, vaid õppida näidete põhjal üldistama ennustusi varem nägemata tuleviku andmetele. Masinõppe tulemusi on vaja rakendada seni veel nägemata andmetel ehk testandmetel.[35]

Tehisintellekti arendamisel kasutatakse masinõppe kolme peamist haru: juhendatud õpe ehk induktiivõpe[36] (*supervised learning*), juhendamata õpe (*unsupervised learning*) ja stiimulõpe (*reinforcement learning*).[37] Juhendatud õppe korral on tehisintellektisüsteemile teada nii treeningnäidete tulemused kui ka probleem. Selle kaudu õpetatakse süsteemile vahet tegema erinevate näidete tulemuste vahel.[38] Seega juhendatud õppe korral treenitakse süsteemi tähistatud andmetega, liigitades iga andmepunkti ühte või mitmesse gruppi (näiteks „õunad” või „apelsinid”). Süsteem õpib, kuidas need andmed – treeningandmed – on struktureeritud ning kasutab teadmist uute – testandmete – kategooriate prognoosimiseks.[39] Juhendatud õpet kasutatakse tänapäeval kõige enam näiteks investeerimistrendide ennustamisel ja finantspettuste tuvastamisel, näo- ja hääletuvastuses ning meditsiinis nahavähi diagnoosimisel.[40]

Juhendamata õpet kasutatakse andmetest struktuuri leidmisel – eesmärk on andmed gruppidesse klasterdada ning leida erinevate andmete seast kasulikke näiteid või tehinguid ilma juhendaja varasemate näidete abil.[41] Juhendamata süsteemid püüavad seega ise õppida, vaadates probleeme värske nurga alt ja aidates inimestel neid lahendada. Kontrollimata õpe

---

[34] S. J. Russell, P. Norvig (viide 16), lk 27

[35] F. Anifowose, A. Khoukhi, A. Abdulraheem. Investigating the effect of training–testing data stratification on the performance of soft computing techniques: an experimental study. 2017. Journal of Experimental & Theoretical Artificial Intelligence. VOL. 29, NO. 3, lk-d 518, 533. Arvutivõrgus: https://doi.org/10.1080/0952813X.2016.1198936 (11.02.2019)

[36] M. Koit, T. Roosmaa (viide 8), lk 194

[37] The Royal Society (viide 32), lk 20

[38] M. Aim (viide 9), lk 10

[39] The Royal Society (viide 32), lk 20

[40] E. Brynjolfsson, A. McAfee. Artificial Intelligence, For Real. Harvard Business Review: The Big Idea. 2017. lk 7. Arvutivõrgus: http://asiandatascience.com/wp-content/uploads/2017/12/Big-Idea_Artificial-Intelligence-For-Real_The-AI-World-Confernece-Expo-Decembe-11_13-2017.pdf (08.02.2019)

[41] S. J. Russell, P. Norvig (viide 16), lk 694-695

võib näiteks aidata tuvastada haiguste levikut, hinnata klientide ostukäitumist ja analüüsida väärtpaberite turuhindade muutusi.[42]

Stiimulõpe, mis on masinõppe meetodite puhul kasvavaks trendiks[43], keskendub algoritmi oma kogemustest õppimisele. Tüüpilises tugevdusõppe keskkonnas suhtleb agent end ümbritseva keskkonnaga ja samaaegselt on talle välja pandud auhinna funktsioon, mida ta püüab optimeerida. Näiteks võidakse süsteemi premeerida mängu võitmise eest. Eesmärgiks on agendil õppida oma otsuste tagajärgedest ja sellest, millised käigud olid mängu võitmiseks olulised, arendamaks uusi strateegiaid, mis aitavad saavutada maksimaalset preemiat.[44] Programmeerija määratleb süsteemi hetkeolukorra ja seab talle eesmärgi, loetleb lubatud tegevused ja kirjeldab üksikasjalikult keskkonna elemente, mis piiravad iga tegevuse väljundit. Kasutades lubatud tegevusi, peab süsteem välja selgitama, kuidas saada võimalikult lähedale eesmärgile.[45] Lihtsaim näide stiimulõppest on arvutimängud – masin- ja sügavõppe programmid õpetavad end mängu ise mängima läbi nähtavate pikslite ja mänguskoori teadvustamise.[46]

Kuigi tehisintellekti arendamiseks on mitmeid meetodeid, on masinõpe üks levinumate meetodite hulgas ning nagu eelpool loetletud, on tehisõpe kokkuvõtvalt protsess, millega tehisintellektisüsteem täiustab oma talitlust, omandades uusi teadmisi või uusi oskusi seniseid ümber korraldades.[47] Masinõppe lähenemisviisid on kasulikud mitte ainult tajuülesannete lahendamisel, nagu tekstimõistmine, nägemine ja tuvastamine, vaid ka kõikides sellistes ülesannetes, mida on raske määratleda ja mida käitumise sümboleeskirjadega ole võimalik põhjalikult kirjeldada.[48]

Kuivõrd masinõppelised tehisintellektisüsteemid tuginevad enda töös väga suurele hulgale andmetele, on tähtis mõista, et just andmed ongi need, mis mõjutavad tehisintellekti käitumist kõige enam, seega kui süsteemile etteantavad treeningandmed on kallutatud – pole kas piisavalt täpsed, kõikehõlmavad või on vigased, ei suuda süsteem selliste andmete põhjal hästi üldistada

[42] E. Brynjolfsson, A. McAfee (viide 40), lk 7-8

[43] E. Brynjolfsson, A. McAfee (viide 40), lk 8

[44] The Royal Society (viide 32), lk 20

[45] E. Brynjolfsson, A. McAfee (viide 40), lk 9

[46] M. Aim (viide 9), lk 11

[47] M. Koit, T. Roosmaa (viide 8), lk 194

[48] The European Commission's High-Level Expert Group On Artificial Intelligence (viide 10), lk 5

ja võib teha sootuks ebaõiglaseid otsuseid, nt eelistada ühte isikut teisele või teha kellelegi parem pakkumine ebapiisavate või vigaste andmete põhjal ehk mõjutada automatiseeritud otsustega inimest märkimisväärselt.[49]

1.2. Tehisintellekti ja „*Big Data*" omavaheline seos

Digitaalse ajastu algusest alates on andmete tootmine olnud pidevas kasvus, luues enneolematu hulgal andmeid, mida on võimalik rakendada potentsiaalselt kasulike teadmiste omandamiseks. Digitaalsete andmete suurem kättesaadavus on õhutanud uut mõtteviisi, mille alusel on andmed muutunud teadmiste ressursiks probleemide lahendamisel ning protsesside ja otsuste tõhususe juures ka kvaliteedi parandamisel. Selline uus mõtteviis ja mõtteviisiga kaasnevad ühiskondlikud muutused on toonud omakorda kaasa suurte andmete osaks olevad tehnilised uuendused. Uute ideede loomine ja sellest tulenevate väärtuse kasvatamine andmete kasutamisel nõudis uusi säilitamis- ja analüüsilahendusi. Suured andmed ehk „*Big Data*" on nende arengute tulemus, kuid „*Big Data*" täpne tähendus nagu ka tehisintellekti tähendus varieerub vastavalt kontekstile, milles seda kasutatakse.[50]

Suurtest andmebaasidest teadmiste väljavõtte kontseptsiooni on uuritud aastaid ja sellele on viidatud kui andmeteadusele, andmekaevandusele (*data mining*) või teadmistele andmebaasidest.[51] Andmed on faktide kogum, tegemist on toorainega andmebaasides, mida kasutatakse andmete kaevandamisel. Teadmised on seevastu kasutajate jaoks midagi huvitavat ja tegemist on kindla mustriga, mis on faktide põhjal loodud.[52] Suurandmeid käsitletakse kui iseenesestmõistetavat ainulaadset nähtust, kuid õiguslikust vaatenurgast suurandmete käsitlemine ainulaadse kontseptsioonina eirab tõsiasja, et suurandmete töötlemisel leiavad aset

---

[49] *Ibid*, lk 6.

[50] M. Oostveen. Identifiability and the applicability of data protection to big data. International Data Privacy Law, 2016, Vol. 6, No. 4, lk 299. Arvutivõrgus: https://doi.org/10.1093/idpl/ipw012 (11.02.2019)

[51] *Ibid*, lk 300

[52] B. Custers. Data Dilemmas in the Information Society Introduction and Overview. Raamatust Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. 1. peatükk, vol 3. Springer 2013, lk-d 3-26, lk 10. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)

mitmed erinevad toimingud, mis mõjutavad andmekaitsealaste õigusaktide kohaldatavust suurtele andmetele. Suurandmete töötlus jagab andmetöötluse omandamis-, analüüsi- ja rakendusetappidesse, lihtsustades kompleksset korduvat protsessi ja aidates suurandmete töötlemist protsessidepõhiselt õiguslikult hinnata.[53]

Andmetöötluse esimeses ehk omandamise etapis saadakse andmeid andmesubjektidelt, programmidest või üksustelt, mis suurandmeid haldavad, ning omandamisetapi käigus toimub pidev andmete kogumine. Andmekogumise käigus töötavad iseõppivad algoritmid, mis reageerivad uute andmete sisendile. Andmeid kogutakse otse füüsiliselt isikult kui andmesubjektilt tehingute tegemise käigus või vahetult ja vabatahtlikult loovutamise teel.[54] Tihtipeale loovutatakse enda isiklikke andmeid vastutasuks tasuta teenuse kasutamiseks.[55] Peamiselt sisaldavad küsitavad andmed isiku nime, e-posti aadressi ning sõltuvalt teabe kasutamise eesmärkidest võidakse isikult küsida näiteks ka krediitkaardi numbrit, elukoha andmeid, ametit, hobisid, sünniaega, meditsiinilisi andmeid ja paljutki veel. Levinud on ka inimese kohta kohustuslike päringute tegemine, pakkumaks talle toodet, teenust või määramaks pakutava toote või teenuse hind.[56] Selliseks näiteks võib tuua toote või teenuse ostmise laenuga – andmesubjekt esitab taotluse, ettevõte edastab taotluse vastavale laenupakkujale, kes teostab isiku suhtes krediidivõimekuse hinnangu, määrab tingimused. Andmeid on võimalik omandada ka tehnikatoodete sensorite kaudu[57]; osta andmeid vahendavatelt ettevõtetelt, kes ise andmeid koguvad ärilistel eesmärkidel, eelkõige kolmandatele isikutele müümiseks. Andmete omandamisetappi iseloomustab pidev andmete kogumine edasiste töötlemisprotsesside teostamiseks ja analüüside ressursina.[58]

---

[53] M. Oostveen (viide 50), lk 300

[54] M. Oostveen (viide 50), lk 301

[55] A. Metzger. Data as Counter-Performance: What Rights and Duties do Parties Have? JIPITEC 2 para 1. 2017, lk 2. Arvutivõrgus: https://www.jipitec.eu/issues/jipitec-8-1-2017/4528/jipitec_8_1_2017_metzger_data%20as%20counter-performance.pdf (01.03.2019)

[56] B. Custers (viide 52), lk 8

[57] M. McCole. This Smart Home Kit Relies on Sensors rather Than Cameras. WIRED. 2016. Arvutivõrgus: https://www.wired.com/2016/03/iotcookbook-smartthings/ (10.02.2019)

[58] Suurimate andmevahendajate näited on välja toonud Bernard Marr. Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers. Forbes, 2017. Arvutivõrgus: https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/#5ba8f18c6c27 (10.02.2019)

Suurandmete töötlemise teiseks etapiks on analüüsimisfaas, milles andmed on kas tugevalt seotud üksikisikutega või juba anonüümsed ning analüüs toimub andmebaasi haldamise või andmetöötluse tarkvara abil. Tegemist on laiamahulise etapiga, mis hõlmab nii andmete säilitamist kui ka andmete ettevalmistamist edasiseks analüüsimiseks ja andmekaevanduseks.[59] Andmekaevandust defineeritakse sageli kui automatiseeritud väljavõtet mustritest, mis kujutavad teadmisi andmebaasidest, andmevoogudest ja muudest suurtest andmehoidlatest. Erinevalt masinõppest, mille eesmärk on sooritada ülesanne, on andmekaevanduse eesmärgiks leida teadmisi erinevatest andmetest.[60] Andmete grupeerimiseks ja mustrite leidmiseks kasutatakse peamiselt kolme meetodit: klasterdamine, klassifikatsioon ja regressioon. Klasterdamine tähendab andmete kirjeldamist läbi sarnaste omadustega rühmade moodustamise. Klassifitseerimine tähendab andmete kaardistamist mitmesse eelnevalt määratletud klassidesse ning regressiooni kasutatakse andmete kirjeldamiseks matemaatiliste funktsioonidega.[61] Need meetodid genereerivad ise hüpoteese ning testivad seatud hüpoteese olemasolevate andmetega.[62] Suurandmed on suunatud eelkõige trendide, mudelite ja seoste analüüsimiseks, mitte aga konkreetsete üksikisikute analüüsimiseks. Seetõttu ei töödelda sageli näiteks nimede või asukoha teavet ning andmed pseudonümiseeritakse või anonüümiseeritakse turvalisuse ja andmekaitse kaalutlustel.[63]

Andmekaevanduse kõrval eksisteerib teine suurandmete kontseptsiooni haru nagu profileerimine, mis tähendab profiilide loomise protsessi ning tegemist on andmekaevanduse kõrval veel ühe meetodiga andmete grupeerimiseks ja analüüsimiseks. Profileerida võib nii ettevõtteid, riike kui ka inimesi. Peamiselt on tegemist sellise protsessiga, mis koondab näiteks isikuandmed või isikute gruppide andmed erinevate omaduste põhjal kogumisse. Profileerimist kasutatakse peamiselt sihtrühmade leidmiseks või tuvastamiseks. Andmekaevandus ja

[59] M. Oostveen (viide 50), lk 301

[60] T. Calders, B. Custers. What Is Data Mining and How Does It Work?, lk 28-29. 2. peatükk raamatust "Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases". Springer 2013, vol 3., lk-d 27 - 42. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)

[61] B. Custers (viide 52), lk 9

[62] *Ibid*

[63] M. Oostveen (viide 50), lk 301

profileerimine aitavad töödelda tohutu koguse andmeid, mida inimesel oleks liialt keeruline käsitsi teha. [64]

Kolmandat etappi nimetatakse rakendusfaasiks, kus rakendatakse analüüsietapis saadud teadmisi. Andmete rakendust tehakse kas automatiseeritult või inimeste poolt. Tehtavad otsustused võivad olla suunatud konkreetsele üksikisikule või üldistatud otsused ilma konkreetsele isikule suunamata, kuid selline üldine otsus võib üksikisikut teataval määral siiski mõjutada. Oluline on mõista, et üldjuhul põhinevad sellised üldised otsused andmetel, mis on saadud mitmetest allikatest ilma konkreetse indiviidi isikuandmeteta, tema tuvastamiseta ja tema vabatahtliku panuseta. Paljudel juhtudel piisab väga vähestest andmetest, et inimeste suhtes teha vastavaid järeldusi ja otsuseid, ning oluline on märkida, et rakendusfaasis ei ole suurandmete eesmärgiks isikut otseselt tuvastada.[65]

Suurandmed on oma olemuselt suuremahulised, pidevas ringluses ja mitmekesised infovahendid, mis nõuavad kulutõhusaid ja uuenduslikke infotöötluse vorme, millega on võimalik paremini anda ülevaateid, langetada otsuseid ja automatiseerida protsesse.[66] Suuremahulisus tähistab suurandmete puhul massiivseid andmekogumeid, andmete ringlus ja kiirus on seotud reaalaja andmetega[67] ning mitmekesisuse all peetakse silmas erinevaid andmeallikaid.[68] Kuna andmemahud on tänapäeval niivõrd palju suurenenud, kasutatakse kõikide andmete töötlemisel matemaatilisi algoritme[69], mis lihtsustavad inimeste panust. Andmekaevandus ja seega suurandmete töötlemine kasvas välja sellistest valdkondadest nagu tehisintellekt, statistika ja analüütika.[70] Kuivõrd tehisintellekti masinõppivad algoritmid

[64] B. Custers (viide 52), lk 12-14

[65] M. Oostveen (viide 50), lk 301

[66] Gartner IT Glossary. Big Data. Arvutivõrgus: https://www.gartner.com/it-glossary/big-data (17.02.2019)

[67] Kusjuures tasub märkida siinkohal, et Euroopa Liit on liikumas 5G võrgu kasutuselevõtu poole, mis kiirendab mobiilseid automatiseerituid toiminguid. Vt: https://ec.europa.eu/digital-single-market/en/connected-and-automated-mobility-europe

[68] Information Commisoner's Office. Big data, artificial intelligence, machine learning and data protection. 04.09.2017, lk 6. Arvutivõrgus: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (17.02.2019)

[69] B. Custers (viide 52), lk 9

[70] T. Calders, B Custers (viide 60), lk 28

kasutavad hulgaliselt erinevaid andmeid enda otsuste tegemiseks, peaksid andmed olema kvaliteetsed ja õiged, et ära hoida otsustusprotsessis inimeste diskrimineerimist.[71]

Suurandmetega seotud võimalused näivad lõputud, kuivõrd need aitavad teha teadlikke otsuseid, andes paremat ülevaadet otsuste kohta ja samaaegselt vähendada otsustega seotud riske. Nende kasutamise tulemusena saab säästa ressursse ja kulusid, muuta erinevad protsessid tõhusamaks, saab vältida pettusi ja teha paremaid otsuseid. Kuna suurandmed aitavad leida seoseid suurtes andmemahtudes, siis öeldakse, et suurandmete abil on võimalik vastata ka küsimustele, mida veel ei ole isegi suudetud küsida. Suurandmete probleemilahendamise võimekust tunnustatakse eriti, kui neid kasutatakse kiireloomuliste ühiskondlike probleemide lahendamisel nagu haigused ja tervishoiukulud. Andmed muutuvad varaks ja tekib mentaliteet „mida rohkem andmeid, seda parem".[72] Ühtlasi on andmed teadmistepõhises maailmas muutunud valuutaks, mida saab vahetada klikkide, vaatamiste arvu, reklaamide ja võimu vastu.[73] Sellise põhimõtte kasv ei ole aga inimeste eraelu huvides. Nimelt privaatsus kaitseb üksikisikute eraelu ja teiste inimeste juurdepääsu eest isiklikule sfäärile. Suurandmete kogumine on üldises pildis siiski aga vastuolus isikute eraelu puutumatuse ja isikuandmete kaitsega, kuivõrd andmete töötlemine selles esimeses faasis – omandamisetapis – võib paljastada intiimseid üksikasju inimese elu kohta ning meie teadmata kogutakse võimalikult palju andmeid, sest mida rohkem on andmeid kui teadmisi, seda parem. Samas ka pidev isikuandmete analüüsimine järgmistes töötlemise etappides võib rikkuda mitmeid andmekaitsealaseid põhimõtteid.[74]

Suured andmed moodustuvad inimeste poolt jagatud väikestest andmetest nagu igapäevased arvuti- ja internetipõhised toimingud ja avaldustest, millega soovitakse saavutada tõhusam elu. Sellises mahus andmete kogumise jaoks ei ole aga mitte miski lühiajaline ega triviaalne,

---

[71] T. Calders, I. Žliobaitė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures, lk 55-56. 3. peatükk raamatust "Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases". Springer 2013, vol 3., lk-d 43-57. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)

[72] M. Oostveen (viide 50), lk 302

[73] M. Krenchel, C. Madsbjerg. Your Big Data Is Worthless If You Don't Bring It Into The Real World. WIRED, 2014. Arvutivõrgus: https://www.wired.com/2014/04/your-big-data-is-worthless-if-you-dont-bring-it-into-the-real-world/ (08.03.2019)

[74] M. Oostveen (viide 50), lk 302

suurandmeid kogutakse Facebookis vajutatud „like"-dest, Google'i otsingutest, e-kirjadest, sõnumitest, fotodest, muusika ja videoeelistustest, asukoha teabest, tehtud ostudest, liikumistest. Iga internetis iga tehtav klikk omab olulist rolli ning olgugi, et klõps on inimese jaoks tähtsusetu, suurandmete mõttes annab see aga parema ülevaate inimkäitumisest.[75] Andmed, mida kunagi peeti mitte-isiklikeks toorandmeteks suurandmete kontseptsioonis, näiteks majapidamisarvestites saadavad näidud või GPS-seadmete asukohaandmed, on muutunud masinõppivate algoritmide tõttu isiklikeks andmeteks, sest selliste andmete alusel on tänapäeval võimalik masinõppivaid tehnikaid kasutades isikuid identifitseerida. See tähendab, et igapäevased tegevused, mida inimesed „arukates keskkondades" ette võtavad, jätavad potentsiaalselt varjatult maha endast ka väga isiklikud andmed ettevõtjate kui vastutavate töötlejate jaoks.[76] Selliste andmete analüüsimist võib pidada tihtipeale aga pahaendeliseks, kuivõrd nende töötlemise eesmärk võib ajas muutuda ning hõlmab andmete ootamatut edastamist, kasutades samaaegselt keerulisi algoritme, mis teevad ettenägematuid järeldusi inimestest ja võivad kaasa tuua soovimatuid tagajärgi.[77]

Suurandmeid käsitletakse varana, mida on raske süstemaatiliselt kasutada, kui puuduvad vastavad vahendid andmemahtude töötlemiseks. Tehisintellekti peetakse siinjuures aga andmete väärtuse avamise võtmeks, mida tehnilise mehhanismina toestab ja hõlbustab algoritmide masinõppimine.[78] Suurandmete ja tehisintellekti omavaheline seotus seisnebki seega asjaolus, et iseõppivad algoritmid vajavad õppimiseks andmeid ning mida rohkem on andmeid, seda paremaid lahendusi ja otsuseid saavad algoritmid pakkuda. Kuivõrd andmed ja algoritmid tuginevad otsuste tegemisel suurtest andmemahtudest, milles suures osas töödeldakse isikuandmeid, tekitab tehisintellekti poolt andmete töötlemine mitmeid õiguslikke probleemkohti andmetöötluse vallas. Peamiseks probleemkohaks andmete töötlemisel on suurandmete analüüsi kasutavate ettevõtete jaoks see, kas töötlusprotsesside läbiviimise tulemused on õiglased andmesubjektide suhtes. Õiglase töötlemise peamiseks komponendiks

[75] S. Zuboff. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology (2015) 30, 75–89. lk 79. Arvutivõrgus: https://cryptome.org/2015/07/big-other.pdf (08.03.2019)

[76] L. Edwards, M. Veale. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 2017, Vol. 16, no. 1, lk 34. Arvutivõrgus: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr (01.04.2019)

[77] Information Commisoner's Office. 04.09.2017 (viide 68), lk 19

[78] Information Commisoner's Office. 04.09.2017 (viide 68), lk 8

on läbipaistvuse tagamine ehk teisisõnu küsimus selle kohta, millist teavet omavad inimesed enda andmete töötlemise osas.[79] Käesolev töö analüüsib järgmistes peatükkides läbipaistvuse põhimõtet isikuandmete kaitses, kuid tutvustab enne tehisintellekti „musta kasti" kontseptsiooni.

1.3. Tehisintellekti „musta kasti" kontseptsioon

Ajalooliselt on kõrvuti arenenud kaks intellekti modelleerimise lähenemisviisi – neuroküberneetika ja „musta kasti" küberneetika.[80] Neuroküberneetika aluseks on eeldus, et ainus mõtlemisvõimeline objekt on inimaju, mistõttu tuleb tehisintellekti saamiseks jäljendada inimaju ehitust, püüdes modelleerida inimaju struktuuri nii tarkvaraliselt kui ka riistvaraliselt.[81] Kunstlik närvivõrk on inspireeritud inimaju neuraalsete võrkude struktuurist. Lihtsustatud ajumudel sisaldab suurt hulka neuroneid, mis on omavahel ühendatud keerulises kommunikatsioonivõrgus, mille kaudu aju suudab teostada väga keerulisi arvutusi. Kunstlike närvivõrke võib kirjeldada kui suunatud punktjoonskeemi, kus punktid tähistavad neuroneid ja servad vastavad nende omavahelisele seosele. Iga neuron saab sisendina oma sissetulevate servadega ühendatud neuronite väljundite kaalutud summa.[82] Tehisnärvivõrk kasutab inimajule kohast näidetest õppimise tehnikat. Ta on konfigureeritud spetsiifilise rakenduse jaoks, nt andmete klassifitseerimine või mustrite tuvastamine õppimisprotsessis, mida nimetatakse treenimiseks. Tehisnärvivõrke võib liigitada mitmel alusel. Kui treeningsisend ja -väljund on antud, siis on tegu juhendajaga õppega, vastupidisel juhul juhendajata õppega. Tehisnärvivõrke võib eristada ka vastavalt sellele, kuidas neuronid on omavahel seotud, kuidas nad teevad arvutusi, annavad edasi tegevusmustreid võrgus ja õpivad. Neid on rakendatud mitmesugustele reaalse maailma probleemidele, mida inimesed lahendavad hästi, aga samas ei suuda selgitada, kuidas seda teevad nt mustrite tuvastus ja ennustamine, mis nõuavad andmetes trendide äratundmist. Praegu kasutatakse laialdaselt andmekaevandust, otsimaks trende

[79] *Ibid.*, lk 19

[80] M. Koit, T. Roosmaa (viide 8), lk 9

[81] *Ibid.*

[82] S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press, 2014. lk 268. Arvutivõrgus: https://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning (06.03.2019)

minevikuandmetes selleks, et ennustada tulevikku.[83] Neuroküberneetika eesmärk on seega luua inimajule sarnane tehislik neurovõrk, mis jäljendab täielikul määral inimintelligentsust ja mõtlemisvõimet.

„Musta kasti" küberneetika väidab vastupidist ja lähtub põhimõttest, et pole tähtis, kuidas funktsioneerib tehisintellekt, vaid on oluline, et see reageeriks sisendile nii nagu inimaju. Eesmärk on töötada välja algoritme selliste ülesannete lahendamiseks, mis inimeselt nõuavad mõtlemisvõimet, arukust, loomingulisust. Väga paljud intellektitehnika meetodid esindavad just „musta kasti" küberneetikat, sealhulgas heuristiline programmeerimine, matemaatilise loogika meetodid (sh teoreemide automaatse tõestamise meetodid), samuti toimivad sel viisil tänapäeva tööstuslikud ekspertsüsteemid.[84]

Termin „must kast" on teadlaste ja inseneride poolt kasutusel erinevates valdkondades ning tegemist on mitmetahulise metafooriga, mis tavapäraselt viitab sisendite ja väljundite läbipaistmatule süsteemile. Tegemist on protsessi või fenomeniga, mille suhtes asjatundjad teavad, mis läheb süsteemi sisse ja mis tuleb süsteemist välja, kuid on teadmatud sellest, millised protsessid toimuvad vahepeal.[85] Masinõppesüsteemid muutuvad „mustadeks kastideks" pärast tugevat treeningprotsessi, mille järel omandavad need täpsed toimimismeetodid, kuid muutuvad raskesti tõlgendatavateks pärast treeningprotsessi lõppemist. Sellised süsteemid võivad anda statistiliselt usaldusväärseid tulemusi, kuid lõppkasutaja ei pruugi olla võimeline selgitama, kuidas vastavad tulemused süsteemi poolt loodi ja millised tunnused olid lõpliku otsuse tegemisel olulised.[86] „Must kast" viitab ühest küljest lennukite, rongide ja autode andmekontrollisüsteemidele ning teisest küljest tähendab see süsteemi, mille töö on salapärane, kuivõrd saab jälgida sisendeid ja väljundeid, kuid ei ole võimalik tuvastada, kuidas sisendist saab väljund[87].

---

[83] M. Koit, T. Roosmaa (viide 8), lk 9, 206,

[84] *Ibid*, lk 9

[85] S. Ranchordás. Book Review: The Black Box Society: The Secret Algorithms That Control Money and Information by Frank Pasquale, MA: Harvard University Press, 2015. Cambridge University Press, 2017, lk 460. Arvutivõrgus: https://doi-org.ezproxy.utlib.ut.ee/10.1017/S1867299X00005894 (06.03.2019)

[86] The Royal Society (viide 32), lk 93

[87] F. Pasquale. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press. 2015, lk 3. Arvutivõrgus http://www.hup.harvard.edu/catalog.php?isbn=9780674368279 (06.03.2019)

Arenevas maailmas ja andmemahtude kasvades ettevõtted ja valitsus jälgivad üha enam inimeste andmeid. Inimestel aga puudub täielikult selge ettekujutus sellest, kui palju neid puudutavast teabest edasi rändab, kuidas teavet kasutatakse või millised on andmekasutuse tagajärjed.[88] Tänapäeva masinõppivad algoritmid on võimelised õppima massilistest andmehulkadest ning hetkel, mil andmed on tehisintellektile antud, on algoritmid tegemas otsustusi kogemuste ja taju baasil nagu inimesedki. See tähendab, et esmakordselt arvutid ei täida enam üksikasjalikke neile eelnevalt kodeeritud juhiseid, vaid suudavad jõuda dünaamiliste probleemide lahendusteni, mis põhinevad andmemudelitel, mida inimesed ise tajuda ei suuda. „Musta kasti" käsitluse järgi muutuvad keerulised algoritmid mustadeks kastideks, kui nende otsuste protsess muutub keeruliseks algoritmide loojatele endale.[89] Iseõppivad algoritmid võivad oma ülesehituse poolest olla sama keerulised kui inimaju, mistõttu ainuõiget ja otsest viisi tehisnärvivõrkude otsustusprotsesside kaardistamiseks ei ole ja seetõttu puudub täielik arusaam, kuidas programm otsustusi ja ennustusi teeb. Kui tehisintellektiprogramm on must kast, siis otsustab ja ennustab ta nii nagu teevad seda inimesed, kuid tehisintellektil puudub vastupidiselt inimmõistusele võimekus edastada põhjendusi ja argumenteerida selle üle, kuidas ta otsuseni jõudis. Kunstlikult loodud intellekti mõtlemisprotsess võib baseeruda mustritel, mida inimmõistus ei suudagi üldse tajuda.[90]

Musta kasti kontseptsioon tõstatab aga mitmeid küsimusi ja sellest tulenevalt eristatakse kolme musta kasti:

1. Organisatsiooniline „must kast" – iseõppivaid algoritme rakendavad enamasti eraõiguslikud üksused, mille eesmärk on pidev kasumi suurendamine ning mis tegutsevad minimaalse läbipaistvuskohustuse läbi.[91]

[88] *Ibid*, lk 3

[89] Y. Bathaee. The Artificial Intelligence Black Box And The Failure Of Intent And Causation. Harvard Journal of Law & Technology. Volume 31, Number 2. 2018, lk 891. Arvutivõrgus: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

[90] *Ibid.*, lk 892-893

[91] G. Noto La Diega. Against the Dehumanisation of Decision-Making. 2018, lk 9-10. Arvutivõrgus: https://www.jipitec.eu/issues/jipitec-9-1-2018/4677/JIPITEC_9_1_2018_3-34 (14.03.2019)

2. Tehniline „must kast" - tehislik intelligents muudab otsuste põhjendatuse sisuliselt raskeks enda keerulise ülesehituse, iseõppimise ja selgituste puudumise tõttu[92] ning seega algoritmi avamiseks tuleb kasutada tehnilisi meetmeid.
3. Õiguslik „must kast" – seostub eelkõige intellektuaalomandi valdkonnaga, tekitades vastuolu isikuandmete kaitse tagamisega[93], peamiselt seostub andmekaitsest tuleneva läbipaistvuse põhimõtte ja ärisaladuse salajasuse vastuoluga, muutes võimatuks „musta kasti" avamise.

Õiguskirjanduses on räägitud sellest, et tänapäeval elame „musta kasti ühiskonnas", kus varjatud algoritmid määravad meie maine, otsustavad ettevõtete saatuse üle või sootuks hävitavad majanduse. Digitaalsed seadeldised ja võrgupõhised infrastruktuurid, mis on varustatud salajaste ja läbipaistmatute omandiõigusega kaitstud algoritmidega, kontrollivad üha rohkem ühiskonna igapäevaelu.[94] Otsused, mis põhinesid varem inimeste osalusel, tehakse nüüd automatiseeritult, kusjuures tarkvara kodeerib tuhandeid reegleid ja juhiseid ning talle antud andmeid vaid murdosa sekundi jooksul[95]. Kõik, mis me teeme veebis ja oma igapäevases elus, kasutades nutikaid tehnikaseadmed, jätavad maha jälje ja kõikide inimeste tegevus on kellegi teise poolt jälgitav.

Käsitledes tehisintellekti kui „musta kasti", taandub peamine probleemkoht selle kontseptsiooni puhul läbipaistvuse küsimusele. Algoritmid on juba oma olemuselt läbipaistmatud – nende otsuste tegemise kriteeriumid on varjatud koodide looriga, mida me ei suuda kergesti lugeda ega mõista; nad on dünaamilised oma võimetes areneda vastavalt erinevatele andmemustritele. Algoritmid võivad olla kaitstud ärisaladusena või matemaatiliselt nii keerulised, et nende õppimisvõime on meie jaoks mõistetamatu, mistõttu tuleb reguleerida algoritmilist õiguskaitset.[96]

---

[92] D. Castelvecchi. Can we open the black box of AI?. Nature, 2016. Arvutivõrgus: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731 (14.03.2019)

[93] G. Noto La Diega (viide 91), lk 10

[94] M. Perel, N. Elkin-Koren. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. Florida Law Review, vol 69. 2017. lk 182, 183. Arvutivõrgus: www.floridalawreview.com/wp-content/uploads/Perel_Elkin-Koren.pdf (14.03.2019)

[95] F. Pasquale (viide 87), lk 8

[96] M. Perel, N. Elkin-Koren (viide 94), lk 181, 185.

Euroopa Liidu nägemus on innovatsiooni levikut toetada ja tehisintellekti valdkonna arendamise investeeringuid tõsta[97], mis näitab, et tehisintellektil põhinevad süsteemid ei kao tänapäeval ega tulevikus kuskile. Sellest tulenevalt on astunud Euroopa Liit ka ühe sammu edasi, kaitstes isikute privaatsfääri andmekaitseliste reeglite kehtestamisega, milles läbivaks ja üheks peamiseks põhimõtteks on isikute õigus andmete töötlemise läbipaistvusele ja õigus saada teavet sellest, kuidas ja mis eesmärkidel andmeid töödeldakse.

Tehisintellekt juriidilise must kastina sõltub peamiselt ettevõtete poolt intellektuaalomandi kasutamisest (andmebaasid, ärisaladused jne) ning sellega sarnastest õigustest, mida äriühingud omandavad kasutajaandmete kogumisest ja mis ei mahu traditsiooniliste intellektuaalomandi liigituste hulka.[98] See tähendab, et tehisintellekt on kellegi intellektuaalne omand samal ajal, kui läbi 4G või 5G võrgu kogutud kasutajaandmed intellektuaalomandi infrastruktuuri alati ei kuulu ega pole kellegi otsene omand, kuid kui andmed moodustavad andmebaasi, saab andmebaas *sui generis* kaitse.[99] Seega, kui tehisintellekti algoritmid ja kasutajaandmed koondatult andmebaasi on kaitstud nii ärisaladuse kui ka intellektuaalomandi õigustega, tuleb leida tasakaal intellektuaalomandi ja andmekaitse regulatsioonide vahel vastuolu kõrvaldamiseks, kuid sellest kirjutab autor lähemalt 3. peatükis.

[97] Euroopa Parlament. Tööstuse, teadusuuringute ja energeetikakomisjon. Raport tehisintellekti ja robootika valdkonna Euroopa tervikliku tööstuspoliitika kohta (2018/2088(INI)). 30.01.2019. Arvutivõrgus: http://www.europarl.europa.eu/doceo/document/A-8-2019-0019_ET.html (16.03.2019)

[98] G. Noto La Diega (viide 91), lk 12

[99] B. Lundqvist. Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. Faculty of Law, University of Stockholm. Research Paper No. 1/2016, lk 10, 13. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2891484 (17.03.2019)

2. TEHISINTELLEKT JA ISIKUANDMETE TÖÖTLEMINE

2.1. Isikuandmete kaitse regulatsioon ja isikuandmed andmetöötluses

2018. aastal kutsus Eesti Vabariigi Riigikantselei kokku ekspertrühma, kelle ülesandeks sai koostada tehisintellektide ehk krattide kasutamise strateegia ning tehisintellekti reguleeriv seaduseelnõu.[100] Euroopa Liidul on samuti nägemus reguleerida tehisintellektisüsteeme eetikakoodeksite ja seadusloomega ning seeläbi suurendada valdkonnapõhiseid investeeringuid, ulatumaks Ameerika Ühendriikidega samaväärsele tasandile ja jõudmaks tehnoloogilise arengu esirinda Aasia ja Põhja-Ameerika kõrval.[101] Liit ei ole aga unustanud, et valdkonna peamine murekoht seisneb isikuandmete töötlemisel, mistõttu on astutud esimene suur samm tagamaks kodanike kaitse nende põhiõigusele – privaatsusele – läbi isikuandmete kaitse üldmääruse.[102]

Euroopa Komisjoni teatisele „Tehisintellekt Euroopa huvides", millele autor viitas eelmises peatükis, vastas Euroopa Majandus- ja Sotsiaalkomitee enda arvamusega, milles selgitas, et tehisintellekt oma olemuselt põhinebki suurte andmekogude kasutamisel ja töötlemisel, mistõttu on Euroopa seadusandja jaoks peamine väljakutse tagada läbipaistev ja reguleeritud juurdepääs lõppkasutajate andmetele.[103] Komitee tõdes ka asjaolu, et mida parem on töödeldavate andmete kvaliteet, seda täpsemad ja tulemuslikumad on tehisintellektisüsteemid. Kusjuures ei tohi unustada asjaolu, et üksikisikuid puudutavad andmed peavad olema hangitud seaduslikult ja isikuandmeid tuleb kasutada viisil, millest asjaomased isikud on teadlikud. Tagada tuleb isikuandmete kasutamine eelnevalt kindlaks määratud ja läbipaistval otstarbel ning kasutaja peab varem olema andnud enda nõuetekohase nõusoleku.[104] Eriti tähtis on samuti tagada, et iseõppivaid algoritme ja andmebaase hallatakse läbipaistvalt ja korrektselt. On näha, et Euroopa Liidu jaoks on äärmiselt oluline, et Euroopa kodanikud saaksid

[100] Riigikantselei (viide 4)

[101] Euroopa Komisjon. Komisjoni teatis (viide 26)

[102] Euroopa Parlamendi ja Nõukogu määrus 2016/679. ELT, L 119, 04.05.2016

[103] Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele „Tehisintellekt Euroopa huvides"" (COM(2018) 237 final). Punkt 4.4. ELT C 440/51. 6.12.2018. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52018AE2369 (16.03.2019)

[104] Euroopa Majandus- ja Sotsiaalkomitee (viide 103), punkt 4.5.

tehisintellektisüsteemide kohta piisava väljaõppe, lihtsa ja arusaadava teabe, ning see aitaks kodanikel kasutada tehnoloogilisi seadmeid või rakendusi vastutustundlikult ja parema teadlikkusega sellest, kuidas nende andmeid kasutatakse ja kuidas seadmed toimivad.[105]

Järgnevalt analüüsib autor, mida on seadusloomes mõeldud läbipaistva andmetöötluse all ja mida on silmas peetud isiku õigusele saada informatsiooni tema andmete töötlemise kohta, kuivõrd tehisintellekti valdkond, nagu juba varem öeldud, on keeruline ja mitte alati selge tehisintellekti loojatelegi olukorras, kus süsteem käitub „musta kastina" ja töötleb otsuste tegemiseks lõpmatul hulgal informatsiooni. Samuti, kuidas suhtuda isiku õigusele saada informatsiooni – kas tegemist on õigusega saada selgitusi?

Eesti Vabariik kuulub aastast 2004 Euroopa Liidu liikmesriikide hulka ja Euroopa Liidu õigus on liikmesriigi õiguse suhtes ülimuslik[106], millest tulenevalt on liikmesriigina asjakohane käesolevas töös võtta analüüsi aluseks nii riigisisesed kui ka liiduülesed õigusaktid. Isikuandmete kaitse peamiseks tugisambaks enne isikuandmete kaitse üldmäärust oli Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ[107], mis andis aluse põhiõiguste harta artiklis 8[108] isikuandmete kaitse õiguse sõnastusele ning suunise, et liikmesriigid peavad tagama inimeste suhtes automatiseeritud otsuste mittetegemist, kui automatiseeritud otsustel on õiguslikud tagajärjed[109]. Isikuandmete kaitse reform oli aga vajalik liikmesriikides erineva isikuandmete kaitse taseme ühtlustamiseks kiiresti areneva tehnoloogia kõrval, kuid probleemaatika ei seisnenud ainult automatiseeritud otsustes ja profileerimises, vaid pigem olulise teabe puudumises algoritmilise loogika kohta, mis profiile loob ja andmesubjekti mõjutab ning

[105] Euroopa Majandus- ja Sotsiaalkomitee arvamus (viide 103), punktid 4.8.-4.9.

[106] Eesti Vabariigi põhiseaduse täiendamise seadus § 2. „Eesti kuulumisel Euroopa Liitu kohaldatakse Eesti Vabariigi põhiseadust, arvestades liitumislepingust tulenevaid õigusi ja kohustusi". RT I 2003, 64, 429; Kommenteeritud väljaanne. „…EL õiguspäraselt vastu võetud ja kehtiv õigus ülimuslik liikmesriigi õiguse suhtes…", kommentaarid nr 3, 16 jt. 2017. Arvutivõrgus: https://www.pohiseadus.ee/index.php?sid=3&p=2 (17.03.2019)

[107] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta - ELT L 281

[108] Euroopa Liidu põhiõiguste harta – ELT C 326/391

[109] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ (viide 107), artikkel 15

seetõttu leidis Euroopa Andmekaitseinspektor, et reformimisel tuleb põhitähelepanu pöörata suurema läbipaistvuse tagamisele.[110]

Regulatsiooni reformimise tulemusena loodi Euroopa Parlamendi ja Nõukogu määrus nr 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, mida kohaldatakse alates 25. maist 2018 ning tegemist on kõikides liikmesriikides vahetult kohalduva ja tervikuna siduva õigusaktiga[111]. Üldmääruse eesmärgiks on aidata kaasa vabadusel, turvalisusel ja õiglusel rajaneva majandusliidu saavutamisele, pöörates rõhku füüsiliste isikute heaolu tagamisele, ühtlustada füüsiliste isikute põhiõiguste ja -vabaduste kaitset isikuandmete töötlemise toimingutel ning tagada isikuandmete vaba liikumine liikmesriikide vahel. Arvestades, et majandus- ja sotsiaalne integratsioon on isikuandmete piiriüleseid andmevoogusid märkimisväärselt suurendanud, on tähtis luua kodanikes kindlusetunne ja usaldus kõrgetasemelise andmekaitsega.[112]

Üldmääruse artikkel 22 annab andmesubjektile õiguse keelduda tema suhtes täielikult automatiseeritud otsuste tegemisest, millel on õiguslikud tagajärjed andmesubjekti elule või mis sarnaselt oluliselt mõjutavad teda, avaldades subjektile märkimisväärset mõju. Kui sellised otsused on lubatud lepingu sõlmimiseks või täitmiseks ja subjekt on andnud andmete töötlemiseks selgesõnalise nõusoleku, peab vastutav töötleja tagama otsuse läbipaistvuse, andes andmesubjektile õiguse otsesele isiklikule kontaktile vastutava töötlejaga, oma seisukohtade väljendamiseks ja otsuse vaidlustamiseks.[113] Täielikult automatiseeritud otsused teostatakse üksnes tehnoloogiliste vahendite abil ilma inimsekkumiseta. Ei saa jätta märkimata, et otsused, mida algoritmid vastu võtavad, võivad põhineda ebatäielikel andmetel, põhjustades diskrimineerivaid otsuseid, mistõttu iga isikuandmete töötlemisviisile kohalduvad artiklis 5 sätestatud põhimõtted: seaduslikkus, õiglus ja läbipaistvus jt. Läbipaistvuse põhimõte on isiku jaoks andmekaitse seisukohast fundamentaalse tähtsusega.[114]

---

[110] Euroopa Andmekaitseinspektori soovitused ELi andmekaitsereformi võimaluste kohta, punkt 3.1. ELT C 301/1, 12.09.2015. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52015XX0912(01)&qid=1554705163152 (17.03.2019)

[111] GDPR, artikkel 99

[112] GDPR, selgitused 6, 10.

[113] GDPR, artikkel 22

[114] Article 29 Data Protection Working Party. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Lk 9. 06.02.2018. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (18.03.2019)

Euroopa Liidu isikuandmete kaitse üldmääruse kõrval jõustus 15.01.2019 Eesti Vabariigis isikuandmete kaitse seadus[115] (edaspidi IKS), mille reguleerimisalasse kuulub füüsiliste isikute kaitse isikuandmete töötlemisel, täpsustades ja täiendades GDPR-i sätteid. IKS § 14 sätestab isikuandmete töötlemise põhimõtted, millest esimesel kohal on seaduslikkus ja õiglus. Järgneb kvaliteedi põhimõte, mille järgi isikuandmed peavad olema piisavad ja asjakohased; andmed peavad olema õiged ja vajaduse korral ajakohastatud.

Sarnaselt GDPR-ga on IKS-s sätestatud turvalisuse põhimõte, mille alusel isikuandmeid töödeldakse viisil, mis tagab nende turvalisuse, sealhulgas kaitseb loata või ebaseadusliku töötlemise eest ning juhusliku kadumise, hävimise või kahjustumise eest, rakendades asjakohaseid tehnilisi või korralduslikke meetmeid.[116] IKS seaduseelnõu seletuskirjas selgitatakse seaduslikkuse põhimõtet selliselt, et töötlemine peab olema „vajalik pädeva asutuse avalikes huvides oleva ülesande täitmiseks liidu või liikmesriigi õiguse alusel süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamise eesmärgil."[117] Seaduse seletuskirja lugedes jääb aga mulje, et Eestis kehtiv isikuandmete kaitse seaduses sätestatud regulatsioonid täpsustavad GDPR-i väheses ulatuses, kuna näiteks seaduslikkuse põhimõtte sisustamisel on lähtutud ainult ühest seaduslikust alusest ja selleks on pädeva haldusorgani poolt andmete töötlemine avalikes huvides oleva ülesande täitmiseks. Erinevalt GDPR artikkel 5 lg 1 punktis c sätestatud „võimalikult väheste andmete kogumise" põhimõttest reguleerib IKS kvaliteedi põhimõtet, mis tähendab, et isikuandmed peavad olema piisavad ja asjakohased ning ei tohi olla ülemäärased andmetöötluse eesmärkide suhtes. Isikuandmeid võib koguda üksnes ulatuses, mis on vajalik määratletud eesmärkide saavutamiseks. IKS kvaliteedi põhimõtet on reguleeritud leebemalt tulenevalt asjaolust, et nii kriminaal- kui ka väärteomenetluses ei pruugi olla teada, millised andmed on taotletava eesmärgi suhtes asjakohased ning seetõttu võib menetlejal olla tarvis koguda andmeid ulatuslikumalt, kui neid tegelikult kasutatakse.[118]

---

[115] Isikuandmete kaitse seadus (IKS). RT I, 04.01.2019, 11

[116] IKS § 14 punktid 1, 3 ja 6.

[117] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde, lk 22. 679 SE, 22.08.2018. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af (18.03.2019)

[118] *Ibid*, lk 23

Turvalisuse põhimõtte all on seadusandja mõistnud, et isikuandmeid tuleb töödelda viisil, mis tagab andmete turvalisuse, kaitseb loata või ebaseadusliku töötlemise eest ja juhusliku kadumise, hävimise või kahjustamise eest. Turvalisuse põhimõtte järgimiseks on vaja kasutada asjakohaseid tehnilisi või korralduslikke meetmeid, millest ühena on seadusandja välja toonud krüpteerimise.[119] Turvalisuse tagamiseks on IKS § 36 alusel vastutaval töötlejal kohustus pidada logisid andmete töötlemisprotsesside kohta ning §-s 37 on reguleeritud isikuandmete töötlemise toimingute liikide registreerimine, tuues välja loetelu, millist teavet registreerima peaks. Nähes, et IKS-is puudub eraldi läbipaistvuse põhimõte, millel on fundamentaalne tähtsus igasuguse andmetöötluse puhul, tuleb lähemalt analüüsida GDPR-i regulatsiooni, millel on liikmeriikide õiguse suhtes otsekohalduv mõju.

IKS § 21 lg 1 keelab sarnaselt GDPR-i artiklile 22 üksnes automatiseeritud töötlusel põhinevat otsust, kui see toob andmesubjektile kaasa teda puudutavaid kahjulikke õiguslikke tagajärgi või avaldab talle muud märkimisväärset mõju.[120] Täielikult automatiseeritud otsused on tõenäoliselt keelatud seoses teadmisega, et masinatel pole inimestele omalaadselt teadvust, mis aitab meil talitleda instinktide järgi ja eristada õiget valest. Teadvus puudub ka algoritmilistel süsteemidel – neil on küll võime õppida ja otsuseid langetada, kuid see oskus ja areng tuleneb inimeste poolt etteantud andmete põhjal. Sageli aga arvatakse, et otsustusvõimelistel algoritmidel puudub inimestele sarnane sünnipärane võimekus näha nö pimenurkadesse, mis tingib ka inimeste poolt vastuvõetud otsustes teatud ebaõiglust või diskrimineerimist. Automatiseeritud otsuste tegemisel ei saa tegelikkuses tagada sajaprotsendiliselt õigeid otsuseid, sest algoritmid on keerulised ja tihtipeale läbipaistmatud ning suured andmemahud võivad samuti algupäraselt peegeldada varjatuid sotsiaalseid ja tehnoloogilisi hälbeid ehk andmed ise võivad olla ebakorrektsed.[121]

Põhjuseid, miks algoritmid kallutatud otsustusi vastu võivad võtta, on tegelikkuses veel mitmeid. Näiteks operaatorite jaoks muudavad algoritmiliste süsteemide loomisel valitud disanilahendused otsustusprotsessi läbipaistmatuks ega anna võimalust otsuseid otseselt mõjutada, piirates samal ajal ka disaineri kontrolli algoritmide üle. Süsteemi väljundid võivad

[119] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde (viide 117), lk 23-24

[120] IKS § 21 lg 1

[121] Written evidence submitted by The Alan Turing Institute (ALG0073). 26.04.2017. Arvutivõrgus: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69165.html (18.03.2019)

olla mõjutatud kogutud andmete hälbest ning erinevalt inimestest ei suuda algoritmid teadlikult pöörata tähelepanu andmete ebaõigsusele.[122] Lisaks võivad vead seisneda õppimisalgoritmide seadistamises, mida tehakse kasutajate käitumise testimise tulemusena ning põhjus, miks algoritmid võivad veel valeotsuseid teha, on süsteemide koolitamisel kasutatavate treeningandmete ebatäpsus või andmete aegumine.[123] Algoritmid on disainitud kindla eesmärgi täitmiseks, kuid võivad olla sisestatud süsteemidesse, millel on hoopis teistsugune eesmärk.[124].

Isikuandmete kaitse regulatsiooni kohaselt on isikuandmeteks igasugune teave tuvastatud või tuvastatava füüsilise isiku ehk andmesubjekti kohta. Isikut on võimalik tuvastada otseselt või kaudselt ning eelkõige selliste identifitseerimistunnuste põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal. Isikuandmete üheks liigiks on eriliigilised isikuandmed, millest ilmnevad andmesubjektide rassiline või etniline päritolu, poliitilised vaated, usulised või filosoofilised veendumused, ametiühingusse kuulumine. Eriliigilisteks andmeteks on veel isikute geneetilised andmed, füüsilise isiku kordumatuks tuvastamiseks kasutatavad biomeetrilised andmed, terviseandmed või andmed füüsilise isiku seksuaalelu ja seksuaalse sättumuse kohta. Biomeetrilised andmed on saadavad konkreetse tehnilise töötlemise abil füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta ja mis võimaldavad füüsilist isikut kordumatult tuvastada või kinnitavad füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed. Geneetilised andmed on seotud füüsilise isiku päritud või omandatud geneetiliste omadustega, andes ainulaadset teavet isiku füsioloogia ja tervise kohta ja tulenevad eelkõige isiku bioloogilise proovi analüüsist saadud isikuandmetest.[125] Seega isikuandmeteks on kõik isikuga seonduvad andmed alustades isiku nimest ja isikukoodist ning lõpetades arvutite IP-aadressitega ja sotsiaalmeedia paroolidega. Kõik andmed, mida inimene kasutab internetivõrgus, aitavad isikut tuvastada ja võimaldavad jälgida tema tegevusi, harjumusi ja palju muudki.

---

[122] Written evidence submitted by Dr Alison Powell (ALG0067). 26.04.2017. Arvutivõrgus: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-andtechnology-committee/algorithms-in-decisionmaking/written/69121.html (18.03.2019)

[123] G. Noto La Diega (viide 91), lk 9

[124] A. Powell (viide 122)

[125] GDPR, artikkel 4 ja 9

2.2. „Üksnes automatiseeritud otsused" tehisintellekti mõistes

Tulles tagasi IKS § 21 lg 1 ja GDPR artikkel 22 lg 1 juurde, siis mõlemad sätted keelavad „üksnes automatiseeritud otsused". Üksnes automatiseeritud otsuste tegemise all mõistetakse siinjuures võimet teha otsuseid tehnoloogiliste vahendite abil ilma inimsekkumise ja kaasaaitamiseta.[126] Silmas on peetud ka andmetöötlussüsteeme, mis töötlevaid andmeid algoritmiliste töötlemistoimingutega[127], tehisintellektitehnoloogiad on üheks selliseks võimaluseks. Tänapäeval, kus tehnoloogiline areng on pidev ja seadmed olemuselt muutuvad ühe keerulisemaks, käivad debatid selle üle, kuidas sisustada „üksnes automatiseeritud" otsuseid tehisintellekti musta kastina käitumise korral. Nimelt ühest küljest leitakse, et täielik automatiseeritus peaks katma sellised autmaatsed otsustusprotsessid, kus inimene reaalselt ei mõjuta otsuse tulemust üldse ega hinda tulemust enne selle formaalseks otsuseks kujundamist.[128] Selline lähenemine praktikas tähendab, et kui nt finantsasutus, mis kasutab andmetöötluses algoritmilisi lahendusi kindlustuspakkumise koostamisel, ei panusta ühegi töötaja poolt pakkumise ülevaatamisega, siis pakkumine osutub formuleeritud otsuseks ja ühtlasi täielikult automatiseeritud otsuseks. Kaitsmaks füüsilist isikut tema andmete töötlemisel valeotsuste tegemise eest, mis on põhjustatud näiteks aegunud andmetest, selgitatakse GDPR-is, et automatiseeritud töötlemise korral peab vastutav töötleja kehtestama sobivad kaitsemeetmed, mis hõlmavad andmesubjektile konkreetse teabe andmist ja õigust otsesele isiklikule kontaktile, õigust väljendada oma seisukohta, õigust saada selgitust otsuse kohta ning õigust otsust vaidlustada.[129]

Nii IKS kui ka GDPR lähtuvad „üksnes automatiseeritud" otsuste tegemisel asjaolust, et puudub inimsekkumine algoritmiliste toimingute läbivaatamisel, andes andmesubjektile võimaluse vaidlustada automatiseeritud otsustused, tagamaks algoritmiliste otsuste ülehindamine inimese poolt ja uue otsuse vastuvõtmine[130] ning otsustuse suhtes peaks

---

[126] Article 29 Data Protection Working Party (viide 114), lk 8

[127] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde (viide 117), lk 27

[128] Information Commisioner's Office. Feedback request - profiling and automated decision-making. 28.04.2017, lk 19. Arvutivõrgus: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/feedback-request-profiling-and-automated-decision-making/ (18.03.2019)

[129] GDPR, selgitus 71

[130] GDPR, artikkel 22 lg 3; IKS § 21 lg 2

ülevaadet omama selleks volitatud ja kompetente isik, kes suudaks automaatset otsust muuta[131]. Tehisintellektisüsteemide puhul on inimsekkumise tagamine keeruline seetõttu, et algoritmid õpivad ja otsustavad tihtipeale arvestamata inimeste arusaamist intellekti õppimis- ja otsustamisprotsesside kohta[132] ning inimsekkumine otsusprotsessist ülevaate andmiseks ei pruugi olla üldse praktikas teostatav, sest töötlusprotsess võib hõlmata kolmandate poolte andmeid ja algoritme, mis on kaitstud ärisaladusega, või on algoritmid juba olemuselt läbipaistmatud[133], mistõttu on parralleelse näitena finantsasutuse töötajal võimatu jälgida automatiseeritult kujundatud kindlustuspakkumise koostamist, kui tal puudub teadmine algoritmi toimimisest ja samas puudub tal sellele ligipääs ärisaladuse tõttu.

GDPR selgitab, et andmesubjekti suhtes õiglase ja läbipaistva töötlemise tagamiseks tuleb arvestada isikuandmete töötlemise konkreetseid asjaolusid ja konteksti ning vastutav töötleja peaks kasutama asjakohaseid matemaatilisi või statistilisi protseduure, rakendama tehnilisi ja korralduslikke meetmeid, et korrigeerida eelkõige ebaõigeid isikuandmeid põhjustavad tegurid ja vähendada vigade tegemise ohtu. Isikuandmete töötlemise turvalisus tuleb tagada ennetava toimega.[134] Ebaõigete andmete ja vastavate tegurite korrigeerimine ning hälvete ilmsiks tegemine tähendab ühest küljest läbipaistvuse tagamist, kuid teisest küljest, mida täpsem on algoritm oma olemuselt, seda läbipaistmatum on selle toime, muutes algoritmisiseste korrektuuride tegemise raskendatuks.[135] Tagamaks inimsekkumine masinõppivate algoritmide poolt teostatavates toimingutes, tähendab ettevõtjate jaoks oluliste investeeringute tegemist ja töötajate väljaõppe teostamiseks ressursi leidmist (asjatundjad, aeg jne), et suuta hoida tehisintellekti süsteemide suhtes autoriteet ja kompetents otsuste muutmisel. Kui aga inimene võtab üle automatiseeritud intellekti otsustused või suudab mõjutada masina poolt tehtud otsuseid, muutub ta süsteemi keerukusest hoolimata vastutavaks intelligentse algoritmi poolt tehtud otsuse eest, mis otseselt mõjutavad kedagi õiguslikult.[136] See on aga omaette küsimus,

---

[131] Article 29 Data Protection Working Party (viide 114). 06.02.2018, lk 21

[132] Information Commisoner's Office (viide 68). 04.09.2017, lk 54

[133] C. Kuner, D. J. B. Svantesson, F. H. Cate, O. Lynskey, C. Millard. Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1, lk 2. Arvutivõrgus: https://academic.oup.com/idpl/article/7/1/1/3782694 (18.03.2019)

[134] GDPR, selgitus 71

[135] G. Noto La Diega (viide 91), lk 9

[136] M. C. Elish. Moral Crumple Zones Cautionary Tales in Human-Robot Interaction. Data & Society Research Institute, 03.04.2016, lk 1. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236 (19.03.3019)

kas ettevõtted soovivad nii kulukaid investeeringuid teha enda töötajate kompetentsi tõstmiseks ja kas töötajad on nõus nii suurt vastutust autonoomsete otsustuste suhtes enda peale võtma. Käesoleva töö autor on seisukohal, et kui programmid ja masinad muutuvad tänapäeva maailmas ühe keerulisemaks oma tehnilise võimekuse poolest, siis on varsti ka täiesti võimatu tagada mõjutava tulemusega inimsekkumine algoritmilistesse süsteemidesse, mis aitaks kaitsta üksikisikute õigusi.

2.3. „Õiguslikud tagajärjed" ja „muu märkimisväärne mõju"

Kui GDPR-i artikkel 22 lg 1 sõnastab automatiseeritud otsuste tegemise keeldumise võimaluse olukorras, kus otsus toob andmesubjektile kaasa „teda puudutavaid õiguslikke tagajärgi" või „avaldab talle märkimisväärset mõju", siis IKS § 21 lg 1 täpsustab automatiseeritud otsustuste keelu, kui need toovad andmesubjektile kaasa teda puudutavaid „kahjulikke õiguslikke tagajärgi" või avaldavad talle „muud märkimisväärset mõju". Õiguslik tagajärg peab seega mõjutama andmesubjekti seaduslikke õigusi. Otsused, mis võivad isikule kaasa tuua õiguslikke tagajärgi võib olla mitmeid: näiteks andmepõhised automatiseeritud otsused võivad määratleda isikule kodakondsuse mitteandmise, mis mõjutab aga isiku õiguslikku staatust ja tema õigust hääletada, samuti võib automatiseeritud süsteem võtta vastu otsuse, et isikul keelatakse riiki sisenemine; algoritmilised otsustused võivad tingida lepingulises suhtes lepingu ülesütlemise; seadusega tagatud sotsiaalse hüve saamise üle otsustamine automatiseeritult võib tuua kaasa tagajärjeks isiku jaoks eitava vastuse ja seega hüvest ilmajäämise.[137] Eesti seadusandja on isikuandmete kaitse seaduse eelnõu seletuskirjas selgitanud, et kahjulik õiguslik tagajärg tähendab andmesubjekti jaoks negatiivset õiguslikku tagajärge, mistõttu tekib regulatsioonide erinevus – üldmääruse eesmärk on kaitsta isikut igasuguse õigusliku mõju eest, mis on tekitatud üksnes automatiseeritud otsustega, ning IKS kaitseb isikuid vaid negatiivsete mõjude eest, olles sõnastuse poolest valinud leebema meetodi. Küll aga lugedes seaduse seletuskirja, on selgelt

[137] Article 29 Data Protection Working Party (viide 114). 06.02.2018, lk 21

näha, et IKS regulatsioonid toetuvad paljuski direktiivile nr 2016/680[138], milles on negatiivset mõju mainitud preambuli punktis 38.[139]

Õigusliku tagajärje mõiste on hoolimata regulatsioonide osalisest erinevusest siiski üsna kindel ja määratletud, kuivõrd tagajärg peab mõjutama üksikisikut otse, kuid „märkimisväärse mõju" mõiste jätab palju lahtisi otsi. Kui automatiseeritud tehisintellektid võtavad vastu otsustuse, mis otseselt ei mõjuta ega muuda isiku seaduslikke õigusi ja kohustusi, võib andmesubjekt olla sellegipoolest piisavalt mõjutatud algoritmilisest otsustusest ning saab kaitset GDPR artiklist 22. Märkimisväärne mõju peab olema aga sarnane õigusliku mõju omavale tagajärjele ja piisavalt oluline, et sellele tähelepanu pöörata. Krediidivõimekust hindavad otsused, kliendiandmete põhjal erineva hinnakujunduse otsused, ülikooli sisseastumisavalduse hindamine, mis otsustab, kas isikul on võimalik rakendada enda õigust haridusele, langevad märkimisväärse mõju sfääri.[140] Märkimisväärne mõju võib inimeste jaoks avalduda ka sotsiaalmeediavõrgustiku kasutusõiguse peatamisega, misjärel puudub neil võimalus kasutada sotsiaalvõrgustiku kasutajakontoga ühildatud teisi rakendusi – näiteks, kui isik soovib üles laadida häbistust ja paljastust sisaldavaid teateid, teostab Facebooki algoritmiline süsteem vastava tuvastuse, misjärel Facebooki kollektiiv peatab isikul võimaluse siseneda enda kontole või keelata postituste tegemist.[141] Muu märkimisväärne mõju isikuandmete kaitse mõttes jääb aga seega sisustada kaasusepõhiselt, kuna ühene selgus mõju ulatuse suhtes puudub.

2.4. Läbipaistvuse põhimõte ja andmesubjekti õigus saada selgitusi

Läbipaistvuse põhimõtet on Euroopa Liidu õiguses pikaajaliselt peetud üheks peamiseks õiguse tunnusjooneks, mille eesmärk on tekitada kodanike usaldust automatiseeritud andmetöötluse

[138] Euroopa Parlamendi Ja Nõukogu Direktiiv 2016/680, 27.04.2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist. ELT L 119/89.

[139] Seletuskiri isikuandmete kaitse seaduse eelnõu juurde (viide 117), lk 27

[140] Article 29 Data Protection Working Party (viide 114). 06.02.2018, lk 21, 22

[141] J. York. Getting banned from Facebook can have unexpected and professionally devastating consequences. Quartz Media, 31.03.2016. Arvutivõrgus: https://qz.com/651001/getting-banned-from-facebook-can-have-unexpected-and-professionally-devastating-consequences/ (19.03.2019)

vastu, mis mõjutab kodanikke, andes võimaluse protsesse mõista ja vajadusel vaidlustada. Tegemist on põhimõttega, mis on lahutamatult seotud õigluse ja vastutuse põhimõttega, kuivõrd GDPR artikkel 5 lõikest 2 tuleneb töötleja kohustus olla suuteline tõendama, et isikuandmeid töödeldakse andmesubjekti suhtes läbipaistval viisil ja töötleja tagab töötlemistoimingute läbipaistvusega enda suutlikkust täita GDPR-ist tuleneva kohustuse. Andmesubjektil tekib läbipaistvuse põhimõtte järgimisel aga võimalus end kaitsta ja teostada läbinähtavat kontrolli andmete töötlemise viiside üle. Läbipaistvuse idee on kasutajakeskne ja seda rakendatakse praktiliste nõuetega.[142]

Kuivõrd GDPR ei defineeri regulatiivsetes osades läbipaistvuse põhimõtet, annab üldmääruse informatiivse osa (preambuli) punkt nr 39 selgituse, et füüsiliste isikute kohta käivate andmete kogumine, kasutamine, lugemine või muu töötlemine ja töötlemise ulatus praegu kui ka tulevikus peaks olema isikute jaoks läbipaistev. Läbipaistvuse põhimõte eeldab, et nende isikuandmete töötlemisega seotud teave ja sõnumid on lihtsalt kättesaadavad, arusaadavad ning selgelt ja lihtsalt sõnastatud. Läbipaistvus seostub eelkõige andmesubjektide teavitamisega vastutava töötleja identiteedist ning töötlemise eesmärgist, täiendavast teabest, tagamaks asjaomaste isikute suhtes õiglane ja läbipaistev töötlemine, ning isikute õigusega saada neid puudutavate isikuandmete töötlemise kohta kinnitust ja sõnumeid.[143]

Üldmääruse peatükk III sätestab artiklid, milles läbipaistvuse põhimõte on läbivaks mõisteks. Artikkel 12 kehtestab reeglid artiklites 13 ja 14 osutatavale teabele, artiklites 15-22 sätestatud andmesubjektidega nende õiguste kasutamise kohta suhtlemisel ja artiklis 34 nõutud teavitusele isikuandmetega seotud rikkumisest.[144] Artikkel 12 nõuab, et edastatav teave ja suhtlus andmesubjektiga vastaks järgmistele reeglitele:

- teave peab olema kokkuvõtlik, läbipaistev, arusaadav ja kergesti kättesaadavas vormis (artikkel 12 lg 1);
- teabe andmisel peab olema kasutatud selget ja lihtsat keelt (artikkel 12 lg 1);
- teave tuleb esitada kirjalikult või muude vahendite abil, sealhulgas asjakohasel juhul elektrooniliselt (artikkel 12 lg 1);

---

[142] Article 29 Data Protection Working Party. Guidelines on transparency under Regulation 2016/679, lk-d 4-5. 11.04.2018. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (19.03.2019)

[143] GDPR, selgitus 39

[144] GDPR, artikkel 12. *Inglisekeelne redaktsioon*

- teabe võib esitada ka suuliselt tingimusel, et andmesubjekt seda taotleb ning isikusamasust tõendatakse muude vahendite abil. (artikkel 12 lg 1);
- teavet on andmesubjektil võimalik saada tasuta (artikkel 12 lg 5)[145]

IKS § 27 sätestab andmesubjekti õiguste teostamise korra, kohustades vastutavat töötlejat sarnaselt GDPR-ga vastama andmesubjekti taotlusele kokkuvõtlikus, arusaadavas ja hõlpsasti kättesaadavas vormis, kasutades selget ning lihtsat sõnastust.[146] Isikuandmete kaitse üldmääruse järgi ei saa andmetöötlust pidada õiglaseks ja läbipaistvaks, kui vastutav töötleja ei võimalda andmesubjektile temalt andmete kogumise hetkel teavet kolmes aspektis. Esiteks peab töötleja tegema teatavaks, et andmetöötlemisel kasutatakse algoritmilist otsustust, teiseks tuleb teavitada subjekti masinõppivate algoritmiliste järelduste tegemise protsessi loogikast. Kolmandaks tuleb isikuandmete kaitse regulatsioonist kohustus avada algoritm, et anda tähendusrikast sisulist teavet sellise töötlemise tähtsusele ja kavandatavate tagajärgede kohta andmesubjekt suhtes.[147]

Üldmääruse artikkel 13 lg 2 punkt f sätestab, et õiglase ja läbipaistva töötlemise tagamiseks tuleb andmesubjektile temalt isikuandmete saamise hetkel esitada teave automatiseeritud otsuste või tehtud otsuste puhul sisuline teave otsustuste tegemisel kasutatava loogika ja selle kohta, millised on sellise isikuandmete töötlemise tähtsus ja prognoositavad tagajärjed andmesubjekti jaoks. Teavitamiskohustust otsustuste sisulise loogika ja prognoositavate tagajärgede kohta tuleb andmesubjektile esitada ka olukorras, kus andmed ei ole kogutud isikult otse. Regulatsioon tuleneb artiklist 14 lõike 2 punktist g ning täiendavalt on sellises olukorras vastutaval töötlejal kohustus andmesubjekti informeerida tema andmete töötlemisest mõistliku aja jooksul pärast isikuandmete saamist, kuid hiljemalt ühe kuu jooksul; või kui andmeid kasutatakse subjekti teavitamiseks, siis andmesubjekti esmakordse teavitamise ajal; või kui isikuandmeid kavatsetakse avaldada kolmandale osapoolele, siis hiljemalt andmete esimese avaldamise ajal.[148] Lisaks andmesubjekti õigusele saada teavet tema suhtes töödeldavate andmete kohta, on isikul õigus tutvuda isikuandmete ja automatiseeritud otsustega ning otsuste

[145] Article 29 Data Protection Working Party (viide 142). lk 6-7

[146] IKS § 27 lg 1

[147] G. Noto La Diega (viide 91), lk 22

[148] GDPR, artikkel 14 lg 3 punktid a)-c)

taga peituva sisulise teabega kasutatava loogika kohta, töötlemise tähtsuse ja isikule prognoositavate tagajärgede kohta.[149]

Et teave oleks esitatud kokkuvõtlikul ja läbipaistval viisil, peab esitatud teave ja subjektiga suhtlus olema tõhus ning konkreetne. Seetõttu tuleb isikuandmeid käsitlevad ja privaatsust puudutavad sätted näiteks veebipõhises keskkonnas eraldada lepinguliste tingimuste sätetest ja üldistest kasutustingimustest, võimaldades isikul tõhusalt üles leida teda puudutavate andmete töötlemisega seotud sektsioon ilma, et subjekt peaks mahukatest terviktekstides nimetatut otsima. Arusaadavuse mõiste isikuandmete töötlemisel tähendab, et teavet peab mõistma ja teave peab olema arusaadav sihtrühma keskmisele liikmele. Läbipaistvuse tagamisel on keskseks kaalutluseks asjaolu, et andmesubjektil oleks võimalik juba eelnevalt kindlaks määrata, milline on andmete töötlemise ulatus ja tagajärjed, ning talle ei tohiks hiljem üllatusena tulla see, kuidas on tema andmeid töödeldud.[150] Sisulise ja tähendusrikka teabe esitamine andmesubjektile automatiseeritud otsustuste loogiliste protsesside kohta tähendab kokkuvõtlikult, et tegemist peab olema teabega, millest andmesubjekt, kes ei ole arvutiteadlane ega spetsialist selles vallas, võiks olla huvitatud ja et ta saaks ilma olulise pingutuseta saadud informatsioonist aru.[151]

Selge ja lihtsa keele kasutamise nõudel on Euroopa Andmekaitsenõukogu lähtunud sellest, et teave tuleks esitada võimalikult lihtsal viisil, vältides keerulisi lause- ja keelestruktuure. Teave peab olema konkreetne ja lõplik, ei tohiks olla abstraktseid sõnastusi[152] ega erinevalt tõlgendatavaid lauseid. Eelkõige peaksid olema selged isikuandmete töötlemise eesmärgid ja õiguslik alus.[153] Seega, kui lähtuda andmete töötlemisel lihtsast keelest ning arusaamast, mis keskmine tehniliste teadmisteta isik võiks omada, siis algoritmiline läbipaistvus ei ole tagatud näiteks olukorras, kus tehisintellekti kasutatavat algoritmi sisaldav tehniline dokument kirjeldab algoritmi töövõimet ja töötlemise protsessi matemaatiliste valemitena. Artikkel 29

---

[149] GDPR artikkel 15 lg 1 punkt h

[150] Article 29 Data Protection Working Party (viide 142), lk 7.

[151] G. Noto La Diega (viide 91), lk 23

[152] Euroopa Komisjon. Kirjuta selgelt. EU publications, 16.03.2011. „Konkreetne sõnum on selge, abstraktne keelekasutus võib jääda ähmaseks ja mitmeti tõlgendatavaks." Arvutivõrgus: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5/language-et (19.03.2019)

[153] Article 29 Data Protection Working Party (viide 142), lk 8

töörühm leiab, et vastutav töötleja peaks leidma lihtsaid viise selgitamaks algoritmiliste otsustuste langetamiseks kasutatavaid aluspõhimõtteid ja kriteeriume, kuivõrd isikuandmete kaitse üldmääruse järgi peab andmetöötleja võimaldama tähendusrikast informatsiooni algoritmi poolt kasutatava loogika kohta ilma algoritmi täieliku avaldamiseta.[154]

Arvestades tehisintellekti algoritmide keerukust nende iseõppiva võime tõttu, võib juhtuda, et andmesubjektile ei olegi üldse võimalik algoritmilisi protsesse selgitada talle arusaadaval viisil, kuid sellegi poolest on töötlejal kohustus anda endapoolselt mõistlik panus informeerimaks tavainimest võimalikult lihtsalt andmetöötluses kasutatavatest kesksetest põhimõtetest.[155]

Leides, et isikuandmete töötlemisprotsessid peavad olema läbipaistvad, tagamaks õiglane andmetöötlus ja otsuste tegemine, kerkib üles järgmine õiguslik küsimus: kas läbipaistvuse põhimõtet järgides ettevõtjate kohustus jagada informatsiooni tähendab oma olemuselt üksikisiku jaoks õigust saada selgitusi?

Õiguskirjanduses on käimas mitmed debatid selle küsimuse üle. On väidetud, et üldmääruse raamistik annab andmesubjektile õigusliku aluse saada selgitusi tehisintellekti algoritmiliste süsteemide poolt langetatud automatiseeritud otsuste kohta või vähemasti otsuse taga peituva loogika kohta ja sellest tulenevalt ka õigust selgitustele üldises mõttes[156]. Õigust selgitustele peetakse kui ideaalseks vahendiks suurema algoritmilise läbipaistvuse ja vastutuse tagamisel, kuid GDPR regulatiivses osas puudub vastav selgitamiskohustuse mõiste enda konkreetses tähenduses – GDPR-i artikkel 22 kui ka IKS § 21, mis automatiseeritud otsustuse suhtes asjakohased on, ei reguleeri selgitamiskohustust, vaid annavad üldise õiguse mitte olla automatiseeritud otsuste subjektiks ning õiguse vastutava töötlejaga kontaktiks otsuste vaidlustamise eesmärgil. Õigus saada selgitust, kuidas algoritmid otsuseid vastu võtavad ja milliseid andmeid selleks kasutavad, tuleneb GDPRi toetavas preambuli osas punktis 71, mis

[154] Article 29 Data Protection Working Party (viide 114), lk 25

[155] G. Noto La Diega (viide 91), lk 23

[156] A. D. Selbst, J. Powles. Meaningful information and the right to explanation. International Data Privacy Law, 2017, Vol. 7, No. 4. Arvutivõrgus: https://doi.org/10.1093/idpl/ipx022 (20.03.2019)

ei ole aga õiguslikult siduv[157], kuid mis annab riikidele tõlgenduse ja suunised isikuandmete kaitse regulatsioonide kohaldamiseks.[158]

GDPRi artikli 13 lõige 2 punkt f, artikli 14 lõige 2 punkt g ja artikli 15 lõige 1 punkt h, kõrvuti IKS § 21 lõikega 1, nõuavad vastutavatelt töötlejatelt teabe esitamist andmesubjektidele automatiseeritud otsuste tegemise kohta või vähemalt sisulise teabe esitamist automatiseeritud otsuste tegemisel kasutatud loogika kohta, viidates samal ajal artiklile 22 lõigetele 1 ja 4. Artikli 22 lõiked 2–4 täpsustavad piiratud asjaolusid, mille puhul on lubatud automatiseeritud otsuste tegemine, ning nähakse ette ettevõtjatele asjakohaste kaitsemeetmete rakendamine, kui automatiseeritud otsuste tegemine on lepinguliselt vajalik või kui on saadud sellekohane nõusoleku andmesubjektilt, andes samaaegselt andmesubjektidele võimaluse oma õigusi ja vabadusi ning õigustatud huve tõhusalt kaitsta. Ühe kaitsemeetmena peetakse silmas otsesest isiklikku kontakti vastutava töötlejaga otsuse vaidlustamiseks[159]. Otsuse vaidlustamine annab isikule võimaluse inimsekkumisele automatiseeritud otsusega mittenõustumisel. Vastutava töötleja poolt kaitsemeetmete rakendamine praktikas võib osutuda raskendatuks, sest tihtipeale disainitakse ja kavandatakse masinõppeprotsessid kolmandate osapoolte poolt, mitte aga vastutava töötleja enda poolt, mistõttu ka algoritmi sisendandmed võivad olla saadud mitmetelt erinevatelt andmepakkujatelt ja iseõppivad protsessid võivad töötada pilvekeskkonnas, mis on samuti mitme teenusepakkujaga soetud. Sellest tulenevalt võib vastutaval töötlejal esineda raskusi asjakohaste tehniliste ja korralduslike meetmete rakendamisega, mida GDPR nõuab andmekaitse põhimõtete, sh läbipaistvuse järgimiseks.[160]

Üldmääruse mittesiduv põhjendus nr 71 sisaldab andmesubjekti õigust saada selgitusi automatiseeritud otsuste tegemisel ning nimetatud preambuli punkt omab olulist rolli

---

[157] T. Klimas, J. Vaičiukaitė. The Law of Recitals in European Community Legislation. ILSA Journal of International & Comparative Law, Vol. 15, 2008. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604 (25.03.2019)

[158] Written evidence submitted by The Alan Turing Institute (viide 121)

[159] Kusjuures GDPR-i inglisekeelses versioonis on sõnastatud nimetatud kaitsemeede „at least the right to obtain human intervention on the part of the controller" ehk isikul on õigus vastutava töötleja poolt otsuste tegemise inimsekkumisele. Regulation 2016/679 Of The European Parliament And Of The Council. EN L 119/1. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

[160] D. Kamarinou, C. Millard, J. Singh. Machine Learning with Personal Data. Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016, lk 13. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811 (25.03.2019)

üldmääruse regulatiivsete osade tõlgendamisel ja toetab artiklite 13-15 ja 22 sätestatud andmesubjekti tõhusat õiguste kasutamist, kuid asjaolu, et nimetatud sätted selgituskohustust ettevõtjatele ei anna, annab riigisiseselt võimaluse selgituskohustuse määramise üle otsustada. Eesti isikuandmete kaitse seadus säärast kohustust ei tunne, vaid sätestab teavitamiskohustuse ja seega on kohtute töö sisustada selgitamiskohustuse ulatust. Leitakse, et informatsiooni jagamise kohustus on leebem versioon selgitamiskohustuse olemusest, kuivõrd hõlmab endas sisulise teabe jagamist tehisintellekti poolt kasutatava loogika ja selle kohta, millised on sellise töötlemise tähtsus ja prognoositavad tagajärjed.[161]

Teisest küljest leitakse, et isikuandmete kaitse regulatsioon selgitamiskohustust ei sätesta, kuna selgitamiskohustus tuleneb regulatsiooni mittesiduvast osast ja informatsiooni jagamise mõiste täies ulatuses selgituste andmist ei sisalda. Seda on väljendanud ka Artikkel 29 töörühm, et andmesubjektile informatsiooni jagamise kohustus ei tähenda ilmtingimata üksikasjalikku samm-sammulist selgitust automatiseeritud otsuste tegemise loogika kohta ja vastavat teavet võiks olla esitatud ilma algoritmi täielikult avamata, kuid teavitus võiks sisalda üldist sisulist ülevaadet andmesubjekti jaoks arusaadavalt[162]. Leitakse ka, et vajadusel tuleks andmesubjektile võimaldada algoritmi kirjeldus, kui see on vajalik andmesubjekti jaoks eksperthinnangu tegemiseks ja algoritmilise otsuse seaduspärasuse hindamiseks.[163] Ollakse seisukohal, et kuivõrd seadusandlusest tuleb isiku õigus saada informatsiooni asjaolu kohta, kas tema andmeid töödeldakse ja milliseid andmeid töödeldakse, siis ei ole ettevõtjad kohustatud rohkemat põhjalikku informatsiooni täiendavate selgitustega masinõppivate süsteemide kohta andma, vaid piisab masinõppiva algoritmi andmetöötlusprotsessis kasutatavatest üldistest põhimõtetest, mille puhul tehisintellekti lahtiharutatud funktsionaalsuse kirjeldus oleks seejuures üleliigne.[164]

[161] A. D. Selbst, J. Powles (viide 156), lk 242

[162] Article 29 Data Protection Working Party (viide 114), lk 25

[163] M. Veale, L. Edwards. Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. Computer Law & Security Review. Volume 34, Issue 2, 2018, 398-404, lk 400. Arvutivõrgus: https://doi.org/10.1016/j.clsr.2017.12.002 (25.03.2019)

[164] S. Wachter, B. Mittelstadt, L. Floridi. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 2017, Vol. 7, No. 2. Arvutivõrgus: https://academic.oup.com/idpl/article-abstract/7/2/76/3860948 (25.03.2019)

Olukorras, kus üldmääruse regulatsioon on selgituskohustuse ja selgituse saamise õiguse osas ebaselge, tekitades õiguskirjanduses konfliktseid arusaamu selgituskohustuse olemasolust ja ulatusest, annab see liikmesriikidele võimaluse aga vastavat mõistet täiendada või täpsustada. Läbipaistvuse põhimõtet selgituskohustuse ulatuses ei ole Eestis jõustunud IKS täpsustanud, mistõttu leiab käesoleva töö autor, võttes arvesse teabe esitamise kohustust nii riigisiseses kui ka üldmääruses sätestatud korras, et informatsiooni andmise klausel mõlemas õigusaktis on siiski võrdsustatav ettevõtete kui vastutavate töötlejate selgitamiskohustusega ja andmesubjekti õigusega saada selgitusi. Nimelt seetõttu, et esiteks mõlemad õigusaktid sisaldavad loetelusid, millist teavet on ettevõtjad kohustatud esitama ja millist lisateavet on andmesubjektil õigus saada. Näiteks IKS § 23 lg 1 p 5 alusel, kui seaduses on sätestatud kohustus teavitada andmesubjekti tema isikuandmete töötlemisest, annab vastutav töötleja vajaduse korral muu lisateabe, IKS § 25 lg 1 alusel on isikul õigus nõuda vastutavalt töötlejalt teda puudutavate ebaõigetel faktidel põhinevate isikuandmete parandamist. Muu lisateabe alla võib kuuluda sellises ülesehituses ka tehisintellekti poolt teostatavate funktsioonide kirjeldused, mis sisaldavad algoritmiliste otsustuste üksikasjalikku selgitust. Üksikisikul ei ole võimalik aga nõuda ebaõigete andmete põhjal tehtud otsuste parandamist, kui ta ei tea, milliseid andmeid tehisintellekt enda toimingutes kasutab ja kuidas kasutab, mistõttu teatud puhkudel tuleb iseõppivate algoritmide „musta kasti" kontekstis vastutaval töötlejal teatud ulatuses siiski avada, kui algoritm on õppinud selgeks uued andmed, mida algselt talle ette ei antud.

Teiseks tundub õigusakte lugedes ja eriti üldmääruse selgitusi, mis ei ole siduvad, kuid aluseks tõlgendamisele ja toetavad regulatiivset osa, et selgitamiskohustust ja informatsiooni saamise, –andmise kohustust peetakse täiesti erinevateks enda ulatuse poolest, kuid käesoleva töö autori arvates on nad oma sisult siiski samaväärsed. Tehisintellekti kui automatiseeritud otsuste mõistes on üldmääruse alusel vajalik esitada muuhulgas ka teave otsuse taga peituvast loogikast ning autori hinnangul ei ole võimalik edastada sisulist teavet loogika kohta ilma täiendavate selgitusteta tehisintellekti masinõppivatest protsessidest. Sellise teabe esitamiseks on vaja mõista kõiksugu mehhanisme otsustusprotsessi kohta ja etapiliselt nö lahti harutada algoritm, nägemaks, milliseid etappe iseõppiv algoritm läbis otsuseni jõudmiseks.

Läbipaistva automatiseeritud andmetöötluse tagamisel ei ole aga täit selgust, kuidas läbipaistvus välja peaks nägema. IKS on enda paragrahvides 36 ja 37 selleks ette näinud logimise ja töötlemistoimingute registreerimise. Õiguskirjanduses on räägitud tihti süsteemide lähtekoodide avaldamisest, kuid seda peetakse vaid osaliseks lahenduseks automatiseeritud

otsuste vastutavuse küsimuse juures. Lähtekoodid ei ole tavainimeste jaoks loetavad ning tegelikult eksperdite jaoks tihtipeale raskesti mõistetavad, mistõttu arvutiprogrammide lähtekoodide avalikustamine on väga piiratud viis ennustamaks programmi käitumist. Masinõppivad algoritmid on eriti sobimatud sääraseks analüüsimiseks, kuna loovad analüüsitavate andmete põhjal otsustuspõhiseid reegleid ise.[165]

Käesoleva töö kirjutaja leiab, et läbipaistvuse põhimõte koosneb selgituskohustusest ja õigusest saada selgitusi, kuid arvestades asjaolu, et tehisintellekti poolt tehtavate otsuste tegemise loogikat on äärmiselt keeruline masinõppiva süsteemi puhul selgitada. Kuivõrd tehisintellekt oma loomuselt on kui „must kast" programmeerijatelegi, kes ei oska igakülgselt öelda, milliseid töötlemisprotsesse otsuse tegemisel algoritm läbib, ei ole selgitamiskohustust läbipaistvuse põhimõtte järgimiseks võimalik täita tehisintellektitehnoloogia keerukuse tõttu. Selgituskohustust on võimalik täita juhul, kui tehniliselt arendatakse vastavad meetodid, millega see võimalik oleks.

Ettevõtjatele on selgitamiskohustuse olemasoluga pandud koorem tehisintellekti keeruliste iseõppiva toimega algoritmi taga peituvat loogikat selgitada, kuid õigusliku „musta kasti" avamine tähendab kõige muu juures seda, et andmesubjekti kaitseks avaldatud informatsioon võib rikkuda kellegi intellektuaalomandiõigusi ning tingida ärisaladuse avaldamise, mistõttu tuleb pöörduda ärisaladuse regulatsiooni poole, nägemaks, kuidas andmekaitse ja ärisaladus omavahel suhestuvad.

[165] J. A. Kroll, J. Huey, S. Barocas, E. W. Felten, J. R. Reidenberg, D. G. Robinson, H. Yu. Accountable Algorithms. University of Pennsylvania Law Review, Iss. 3, 2017, Vol. 165: 633, lk 638. Arvutivõrgus: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/ (25.03.2019)

3. TEHISINTELLEKTI KAITSE ÄRISALADUSENA

Tänapäeva ühiskonnas, kus algoritmid teevad otsuseid üksikisiku elu suhtes, töödeldes isiku laenusaamise taotlust ja võttes töödeldud andmete põhjal vastu laenuandmise või keeldumise otsus, kontrollides isikutuvastamise algoritmidega isiku võimalust ületada piiripunkt ja reisida, vaadates läbi organisatsiooni poolt määratud kriteeriumite alusel ametikoha kandidaate ja sõlmida parima parameetritega kandidaadiga automatiseeritult töölepinguid, võimaldavad masinõppivad koodide jadad erasektori ettevõtjatel ja avalik-õiguslikel organitel analüüsida suurandmeid oluliselt lihtsamalt. Erinevaid andmetöötlustehnikaid kasutatakse automatiseeritud otsuste langetamiseks (nt profileerimistehnikad) ning tehisintellekti läbipaistmatus ei ole tingitud üksnes asjaomaste kasutatud tehnikate eripäradest või nende keerulisusest, vaid tehisintellekti läbipaistmatus on tingitud tihtipeale intellektuaalomandiõiguste kasutamisest ja intellektuaalse omandi regulatsiooni vastuolus isikuandmete kaitse reeglitega.[166] Kuivõrd maailmas üha enam panustatakse innovatsiooni levikusse, toetatakse erinevaid huvitavaid uudseid ideid ja tehakse suuri investeeringuid tehnoloogiliste ideede teostamiseks, et tagada konkurentsivõimelisus[167], on oluline kaitsta omandit ning seda nii materiaalse vara kui ka immateriaalse ehk intellektuaalse varana.

Nii nagu Euroopa Liidu õigusaktid sätestavad omandipõhiõiguse[168] sätestab ka Eesti Vabariigi põhiseadus (edaspidi PS) kaks paragrahvi omandi kaitseks. PS § 32 ütleb, et omand on puutumatu, võrdselt kaitstud ning seda võib vabalt vallata, kasutada ja käsutada, kuid ei tohi kasutada üldiste huvide vastaselt. PS § 39 alusel on autoril õigus enda loomingule, kaitstes loometöö looja isiklikke ja temast lahutamatuid ehk isiklikke õigusi. Kui viimases on kaitsealas isiklikud õigused, siis PS § 32 kaitsealas on loometööga seonduvad varalised õigused ning ka need intellektuaalomandi liigid, mis saavad kaitse investeeringuna – andmebaasid ja ärisaladus[169]. Kinnis- ja vallasomandi kõrval seega kaitstakse ka intellektuaalset vara intellektuaalse omandina, mille määratlus tuleneb Ülemaailmse Intellektuaalse Omandi Organisatsiooni asutamise konventsiooni artiklist 2 (viii) – intellektuaalne omand sisaldab

[166] G. Noto La Diega (viide 91), lk 1

[167] Euroopa Komisjoni teatis (viide 26)

[168] Euroopa Liidu põhiõiguste harta (viide 108), artikkel 17

[169] M. Ernits, A. Kelli, P. Roosma. Põhiseaduse § 32 kommentaar 11. - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017; Euroopa Liidu põhiõiguste harta artikkel 17 lg 2 kinnitab, et intellektuaalomandit kaitstakse.

õigusi seoses kirjandus- ja teadustöödega, leiutistega kõigis inimtegevuse valdkondades, kaitstes kõlvatu konkurentsi vastu, ja kõiki teisi õigusi, mis tulenevad intellektuaalsest tegevusest.[170] Intellektuaalomandi erinevaid liike käsitleb intellektuaalomandi õiguste kaubandusaspektide leping (edaspidi TRIPS-i leping), mille järgi tunnustatakse intellektuaalomandina autoriõiguseid ja sellega kaasnevaid õiguseid, kaubamärke, geograafilisi tähiseid, tööstusdisainilahendusi, patente, mikrolülituste topograafiat ning avalikustamata teabe kaitset.[171]

Tehisintellekt oma olemuse tõttu kuulub intellektuaalomandi hulka. Selle loojaks on inimene ehk programmeerija[172], kes enda loometöö tulemusena loob algoritmi, mistõttu tuleb tehisintellekti nimetada teoseks – arvutiprogrammiks[173]. Tehisintellekti algoritm on arvutiprogramm, mis on väljendatud programmeerimiskeelses lähtekoodi vormis.[174] Autoriõiguse seaduse (edaspidi AutÕS) alusel on arvutiprogrammid kaitstavad kirjandusteosena ning autoriõiguslik kaitse laieneb programmi mis tahes väljendusvormile. Oluline on eristada kahte liiki autoriõigusi – isiklikud, mis on autorist lahutamatud, ning varalised õigused, mis on võõrandatavad.[175] Tehisintellekti loojad saavad tehisintellekti kui teose loomisega nii isiklikud kui ka varalised autoriõigused. Vastavalt AutÕS §-le 5 tehisintellekti taga peituvad ning algoritmis sisalduvad toimimise põhimõtted ja andmetöötluse protsessid autoriõiguslikku kaitset eraldiseisvana ei saa, küll aga on võimalik tööpõhimõtteid ja protsesse ehk algoritmi funktsioone kaitsta ärisaladusena, samuti on andmebaase võimalik kaitsta ärisaladusega.[176]

Ärisaladuse kontseptsioon sai alguse 19.sajandi keskpaigas, kui hoogustus ettevõtjatevaheline informatsioonivahetus ja anglo-ameerika õigusüsteemis hakati ärisaladust käsitlema erinevate

---

[170] Ülemaailmse Intellektuaalse Omandi Organisatsiooni asutamise konventsioon. 05.02.1994. RT II 1993, 25, 55.

[171] Intellektuaalomandi õiguste kaubandusaspektide leping. RT II 1999, 22, 123, artikkel 1 lg 2.

[172] M. Rosentau. Intellektuaalse omandi õigused infotehnoloogia valdkonnas. Infotehnoloogilise loomingu olemus. Juridica III/2008, lk 171, 179. Arvutivõrgus: http://juridica.ee/article.php?uri=2008_3_intellektuaalse_omandi_igused_infotehnoloogia_valdkonnas_infotehnoloogilise_loomingu_olemus (02.04.2019)

[173] M. Koit, T. Roosmaa (viide 8), lk 18 – „Tehisintellektisüsteemi all mõistetakse arvutiprogrammi, mis modelleerib intellektuaalset tegevust."

[174] M. Rosentau (viide 172), lk 176

[175] Autoriõiguse seadus § 4 lg 3 p 3; §§ 11-13 RT I, 19.03.2019, 54.

[176] M. Rosentau (viide 172), lk 179

õigusdistsipliinide osana. Ärisaladust ja selle lubamatut kasutamist tõlgendati enamasti kõlvatu konkurentsi vormina konkurentsiõiguses, lepingu- ja omandiõiguses kaitsenormidena.[177] Ärisaladuse mõiste on Eesti õigusmaastikul samuti olnud tihedalt seotud konkurentsiõigusega[178], mis on ärisaladuse kaitsmise sidunud kõlvatu konkurentsiga võitlemiseks.

Rahvusvaheliselt on ärisaladuse regulatsioon sätestatud TRIPS-i lepingu artikli 39 lõikes 2, kus ärisaladust on defineeritud kui füüsiliste ja juriidiliste isikute õigust takistada nende seadusliku kontrolli all oleva teabe avaldamist, selle omandamist või kasutamist teiste isikute poolt ilma teabe omaja nõusolekuta viisil, mis on vastuolus ausate kaubandustavadega. Tingimuseks on see, et ärisaladusena kaitstav teave oleks saladus selles tähenduses, et teave ei ole kogumis või üksikosade täpses paigutuses ja kokkupanus üldteada või kergesti kättesaadav isikutele nendes ringkondades, kes tavaliselt sellist laadi teabega tegelevad. Sellisel teabel peab olema kaubanduslik väärtus just tema salajasuse tõttu ning teabe üle seaduslikku kontrolli omav isik on asjaoludest lähtuvalt võtnud vajalikke meetmeid, et hoida teavet salajas.

Ärisaladuseks loeti Eestis varasemalt kehtinud konkurentsiseaduse § 63 lg 1 järgi niisugust teavet ettevõtja äritegevuse kohta, mille avaldamine teistele isikutele kahjustaks selle ettevõtja huve. Eelkõige peeti konkurentsiseaduse järgi saladuseks oskusteavet puudutavat tehnilist ja finantsteavet, kulude hindamise metoodikat, tootmissaladuste ja -protsesside, tarneallikate, ostu-müügi mahtude, turuosade, klientide ja edasimüüjate, turundusplaanide, kulu- ja hinnastruktuuride ning müügistrateegiate kohta käivat teavet.

Ärisaladust on Euroopa Liidu üleselt asutud reguleerima isikuandmete kaitse kõrval ning 2016.aastal võtsid Euroopa Parlament ja Nõukogu vastu direktiivi[179], milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset (edaspidi ärisaladuse direktiiv) ning mille järgimiseks pidid liikmesriigid jõustama vajalikud õigusnormid hiljemalt 9. juuniks 2018. Eesti Vabariik jäi

[177] S. K. Sandeen. The Cinderella of Intellectual Property Law: Trade Secrets. - P.K. Yu (toimet). Intellectual Property and Information Wealth: Issues and Practices in the Digital Age. Volume 2. Patents and Trade Secrets. Westport, Conn, London: Praeger, 2007, lk 400-401

[178] Kuni 17.12.2018 kehtis konkurentsiseaduses § 63, mis sätestas ärisaladuse määratluse. RT I, 26.05.2017, 2.

[179] Euroopa Parlamendi ja Nõukogu direktiiv 2016/943, 08.06.2016,milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset. ELT L 157/1.

nimetatud kuupäevaga veidi hiljaks, kuid 17.12.2018 jõustus ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus (edaspidi EKTÄKS)[180].

Direktiivi kohaselt on ärisaladuseks teave, mis peab vastama järgmistele tingimustele:

- see on saladus selles tähenduses, et see ei ole kogumis või üksikosade täpses paigutuses ja kokkupanus üldteada või kergesti kättesaadav nende ringkondade isikutele, kes tavaliselt kõnealust laadi teabega tegelevad;
- sellel on kaubanduslik väärtus selle salajasuse tõttu;
- selle üle seaduslikku kontrolli omav isik on asjaoludest lähtuvalt võtnud vajalikke meetmeid, et hoida seda salajas.[181]

Ärisaladuse omandamist peetakse seaduslikuks, kui ärisaladust on omandatud iseseisva avastuse või loomise teel; kui on jälgitud, uuritud, demonteeritud või katsetatud toodet või eset, mis on tehtud üldsusele kättesaadavaks või mis on sellise teabe omandaja seaduslikus valduses; töötajatelt teabe saamise teel; kui on omandatud muude tavade teel, mis on konkreetsete asjaolude korral vastavuses ausa kaubandustavaga. Samaväärsed põhimõtted ärisaladuse kontekstis sisalduvad ka ärisaladuse kaitse seaduses.[182]

Hetkel kehtivad õigusaktid ei reguleeri ärisaladuse legaaldefinitsiooni ega sätesta loetelu ärisaladuse kaitse alla kuuluvatest võimalustest, vaid määratleb kolm peamist ja kõige olulisemat aspekti – teave ei ole üldteada, sellel on kaubanduslik väärtus ning seda peab hoidma salajas. Teadmistepõhises majanduses on keskseks väärtuseks oskusteave ja teabe omandamine pakub konkurentsieelist, mistõttu tuleb ettevõtjatel üha enam investeerida oskusteabe arendamisse ja rakendamisse, et pakkuda innovatsioonilisi lahendusi turul. Saamaks investeeringust täit kasu, tuleb tagada omandiõigus enda tulemustele, millega piirata konkurentide juurdepääs ettevõtja jaoks väärtuslikele teadmistele, teenimaks jätkusuutlikku tulu. Direktiivi preambul selgitabki, et ettevõtjate jaoks väärtuslikku oskus- ja äriteavet, mida ei soovita avalikustada, vaid soovitakse hoida konfidentsiaalsena, nimetatakse ärisaladuseks ning selline saladus ettevõtjate poolt on enim kasutatav intellektuaalse loomingu ja innovaatilise oskusteabe kaitsmise viis. Erinevalt muudest intellektuaalomandi liikidest ei eelda ärisaladusega teabe kaitsmine loomingulisuse kriteeriumit nagu autoriõigustega kaitstavate teoste puhul, vaid piisab sellest, et teabel on kaubanduslik väärtus ja teavet hoitakse saladusena.

[180] Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus – RT I, 07.12.2018, 2.

[181] Ärisaladuse direktiiv, artikkel 2 lg 1

[182] EKTÄKS § 5 lg 2

Eesti keele seletav sõnaraamat annab ärisaladuse mõistele määratluse, et tegemist on teabega, mille levimine konkurentide seas võib kahjustada ettevõtte huvisid.[183]

Ärisaladuse direktiivi preambuli punkt 34 selgitab, et direktiiv on loodud põhiõigusi järgides ja arvesse on võetud selliseid põhiõigusi nagu õigust era- ja perekonnaelu puutumatusele, isikuandmete kaitsele, sõna- ja teabevabadust, kutsevabadust ja õigust teha tööd. Samuti ettevõtlusvabadust, õigust omandile, õigust heale haldusele – silmas peetakse õigust tutvuda dokumentidega, järgides seejuures ärisaladust, õigust tõhusatele õiguskaitsevahenditele ja õiglasele kohtulikule arutamisele. Punkti 35 järgi on tähtis, et „järgitaks era- ja perekonnaelu puutumatuse ja isikuandmete kaitse õigusi isiku puhul, kelle isikuandmeid ärisaladuse omaja võib ärisaladuse kaitseks võetavate meetmete puhul töödelda või kes on seotud käesoleva direktiivi kohast ärisaladuste ebaseaduslikku omandamist, kasutamist või avalikustamist käsitlevate kohtumenetlustega ja kelle isikuandmeid töödeldakse." Seetõttu ei tohiks käesolev direktiiv mõjutada direktiiviga 95/46/EÜ sätestatud õigusi ja kohustusi, eelkõige andmesubjekti õigust tutvuda oma töödeldavate isikuandmetega, nõuda nende parandamist, kustutamist või sulgemist, kui andmed on ebatäielikud või ebaõiged, ning asjakohasel juhul kohustust töödelda delikaatseid andmeid vastavalt direktiivi 95/46/EÜ artikli 8 lõikele 5 (direktiiv 95/46/EÜ ei kehti, kuid samad põhimõtted on üle võetud GDPR-i). Lisaks on andmesubjektile antud õigus saada informatsiooni sellest, milliseid andmeid, kuidas, miks ja milliste tagajärgedega töödeldakse.

Sellist tõlgendust järgides tundub üheselt selge, et ärisaladuse kõrval eelistatakse siiski andmesubjektide huve ning justkui tuleks siiski ärisaladus avalda ja ohustada sellega konkurentsivõimalused. Paraku selline lähenemine ei ole aga lihtne, sest ka isikuandmete kaitse üldmäärus sätestab juhise, et andmesubjekti õigus enda andmetele juurdepääsuks ja tutvumiseks ei tohiks kahjustada teiste isikute õigusi ega vabadusi, sealhulgas ärisaladusi ega intellektuaalomandit ning eelkõige tarkvara kaitsvat autoriõigust.[184]

[183] Ärisaladus –M. Langemets jt (toim.). Eesti keele seletav sõnaraamat. Eesti Keele Sihtasutus 2009. Arvutivõrgus: http://www.eki.ee/dict/ekss/index.cgi?Q=%C3%A4risaladus&F=M (03.04.2019)

[184] GDPR, preambuli punkt 63

3.1. Tehisintellekti algoritm ärisaladusena

Ettevõte, kes kasutab enda äriliseks tegevuseks tehisintellekti kui IT-loomingu abi andmetöötluseks, kasvatades konkurentsivõimelisust, omab õiguslikus mõttes intellektuaalse omandina tehisintellekti kasutamiseks varalisi autoriõiguseid. Eesti seaduse järgi peab olema teose autoriks füüsiline isik, seega tehisintellekti loojaks ei saa pidada seaduse silmis ettevõtet, kuid autoriõiguslikust küljest on tehisintellekti loojal autoriõiguseid – eelkõige varalisi õiguseid võimalik üle anda, jagada, litsentsida osaliselt või täielikult ja seda tasu eest või tasuta. Autori varalisi õigusi võib sisuliselt pidada majanduslikeks ehk ärilisteks õigusteks, sest autoriõigusliku kaitse puhul on peamiseks otstarbeks teoste loojatele tasu või hüvitise tagamine. Tehisintellekti lähtekood oma programmeerimiskeelse väljendusena tähistab arvutiprogrammi ja saab kaitse nagu kirjandusteoski, kuid otseselt kirjandusteos see ei ole. Arvutiprogrammide algoritme ja põhimõtteid on võimalik seevastu kaitsta ärisaladusena.[185]

Kui isikuandmete kaitse regulatsioon nõuab, et andmesubjektile tuleb selgitada automatiseeritud otsuste tegemisel peituvat sisulist loogikat, on sellist kohustust vastutavatel töötlejatel keeruline tagada olukorras, kui nende poolt kasutatava masinõppeliste algoritmide toime, põhimõtted, loogika on ärisaladusega kaitstud. Ei ole vahet, kas tehisintellekti loojaks on ettevõtte enda töötajad või on tehisintellekti süsteem kasutusel litsentsi alusel, oluline on siinjuures asjaolu, et esiteks algoritmide loogilistest seletustest on võimatu ettevõtjatel ja ka loojatel aru saada, kui algoritmid õpivad, täiendavad end ja otsustavad iseseisvalt. Teiseks, võib tehisintellekti kasutajaettevõte kui ka intelletki loojad kaitsta algoritmilist mehhanismi ärisaladusena. Ärisaladuse direktiivi kohaselt peab ettevõte võtma kasutusele kõikvõimalikud meetmed ja aktiivselt tegutsema selle nimel, et hoida ärisaladus konfidentsiaalsena. Selgitamaks aga andmesubjektile, kuidas algoritm otsuseid teeb või miks teatud otsuseni jõudis, on ettevõtja sisuliselt rikkunud saladuse konfidentsiaalsena hoidmise kohustust ja seeläbi kahjustab ettevõtte kui ka kellegi teise osapoole ärilisi huve.[186]

---

[185] M. Rosentau. Intellektuaalse omandi õigused infotehnoloogias. Autori varalised õigused. Juridica X/2010, lk 752-753, 763. Arvutivõrgus: http://juridica.ee/article.php?uri=2010_10_intellektuaalse_omandi_igused_infotehnoloogias_autori_varalised_igused (04.04.2019)

[186] Euroopa Komisjon. Commission Staff Working Document. Impact Assessment. Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Brussels,

Eelkõige on oluline hoida tehisintellekti algoritmiliste otsustusprotsesside taga peituvat loogikat saladuses seetõttu, et otsuse tegemise põhimõtete avaldamine võib rikkuda ettevõtte turvakaalutlusi ja võimaldada seeläbi oskuslikumal inimesel manipuleerida otsustusprotsesse, mistõttu on oluline teatud elemente tehisintellektisüsteeme kasutaval juriidilisel isikul hoida konfidentsiaalsena. Eriti omab salajasus tähtsat rolli, kui kaubanduslike automatiseeritud otsuste tegemisel nii sisendina kui ka väljundina kasutatakse tundlikke ja privaatseid isikuandmeid (teisisõnu eriliigilisi isikuandmeid üldmääruse tähenduses), mida pole võimalik üldjoontes ettevõtte ärihuvidest lähtuvalt jagada. Näiteks krediidiasutused hindavad automatiseeritud otsustustena tarbijate krediidi- ja kindlustusriske, mille eesmärk on hinnata midagi otseselt mõõdetamatut – krediidivõimekuse katkemise riski või kindlustuspoliisilt kahju saamise riski. Selliseid andmeid arvutatakse puhverserveri muutujatest nagu tarbija krediidiajalugu, sissetulek või isikuomadused ning kui tarbija, kes mõistab kindlustusmatemaatilisi protsesse, manipuleerides andmetega ja sekkudes süsteemi, väheneb ettevõtte kasumlikkus selliste riskide hindamisel ja tulemused ei ole enam usutavad. Seega konfidentsiaalsus takistab süsteemi strateegiliste manipulatsioonide ja andmete avalikustamise eest.[187]

Isegi, kui andmesubjekt nõuab enda kaitseks andmete kustutamist, parandamist või muud sellist, siis ettevõttel on õigus selgitada, et ärisaladusest tulenevalt ei ole võimalik loogilist sisulist informatsiooni jagada automatiseeritud otsuse tegemise kohta. Kui ettevõtjal on siiski võimalik andmetest või protsessidest lähtekoodi ja algoritmi suhtes läbipaistvalt ülevaadet saada, ei ole välistatud, et muudetud või parandatud andmetega tehisintellekt teistmoodi otsuse vastu võtaks. Tehisintellektisüsteemi lähtekoodi või algoritmi kontrollimine koos sellesse sisestatud andmetega ja vastava keskkonna võimaldamine, milles seda otsuse tegemisel kasutati, ei selgita tõsiasja, et just seda koodi kasutati tegelikult konkreetse tulemuse saamiseks. Projekteerimise tulemusena saadakse ettearvamatuid tulemusi, mis ei ole reprodutseeritavad[188] ja tehisintellekti algoritmid loovad arengu käigus samal ajal uusi koode, mille abil enda otsustusprotsessi täiendavad. Arvutisüsteemid, mis valivad sotsiaalmeedia postituste alusel kasutajatele näidatavaid postitusi või reklaame, värskendavad prognoosimismudelit pärast tehtut otsustust kasutajakäitumise põhjal, kaasates iga vaatlustulemust treeningandmete hulka.

28.11.2013. SWD(2013) 471 final, lk 112. Arvutivõrgus: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2013:0471:FIN:EN:PDF (04.04.2019)

[187] J. A. Kroll jt (viide 165), lk 658

[188] *Ibid* (viide 165), lk 659

Süsteemide lähtekoodi ja andmete tundmine ei ole piisav sellise käitumise kordamiseks või ennustamiseks, millest tulenevalt ei ole isikuandmete kaitse seisukohalt läbipaistvuse tagamine või selgituste jagamine piisav.[189]

Kui ühel päeval otsustab Facebook'i sotsiaalmeediaplatvormi kasutaja uurida, soovides selgitusi, miks tema Facebook'i seinal näidatakse tema jaoks ebameeldivaid uudiseid ja tuttavate postitusi, mida näha ei sooviks või tahaks näha hoopis teatud aspektis tutvusringi muid tegemisi, siis Facebook võib esiteks selliste põhjendustest hoidumiseks öelda, et selliseid valikuid teeb nende poolt kasutatav masinõppeline algoritm, kuid seoses ärisaladusega ei ole võimalik algoritmilist mehhanismi võimalik kasutajatele avaldada. Ühtlasi selleks ajaks, kui Facebook kasutajale selgitusi jagama hakkab, on masinõppeline algoritm täiustanud enda tegevust ja pole võimalik tuvastada, miks sellisel ajahetkel otsustas kasutajale just selliseid postitusi näidata. Facebooki ja paljude teiste ettevõtete algoritmid on tugevalt kaetud saladuse looriga, mis tagab neile konkurentsieelise, jäädes läbipaistmatuks.[190]

Ameerika Ühendriikides on ärisaladuste kohtupraktika arenenud pikaajaliselt ning sealses õiguskorras kaitstakse ettevõtete saladusi tugevalt. Algoritmilisi lahendusi, mis on loodud paljude inimeste koostöö tulemusena ja suureväärtuseliste investeeringutega, kasutatakse sealgi igas valdkonnas, kuid ärisaladuslikule kaitsele ei ole võimalik inimestele tagada mehhanismi läbipaistvust. USA-s määrati kodanikule 6-aastane vanglakaristus ning kohtuotsus tugines osaliselt eraettevõttele kuuluva tarkvara salajase algoritmi poolt koostatud aruandele, mistõttu ei olnud isikul võimalik ka inspekteerida algoritmi poolt tehtud otsust[191]. Ameerika Ühendriikide kuulsaimas kohtuvaidluses Viacomi ja YouTube-i vahel soovis Viacom saada YouTube-i algoritmilist koodi, mis kontrollib nii YouTube-i kui ka Google-i otsingumootorite tulemusi. Kohus keeldus kohustamast algoritmide avalikustamist ja selgitas, et otsingukood on genereeritud tuhandete inimeste töö tulemusena ning pole vaidlustki selles osas, et algoritmil on üüratu kaubanduslik väärtus. Tagades koodile juurdepääs, võiks keegi omandada algoritmi

[189] *Ibid* (viide 165), lk 660

[190] H. Hodson. The secret system controlling your Facebook News Feed. New Scientist, 30.07.2014. Arvutivõrgus: https://www.newscientist.com/article/mg22329804-200-the-secret-system-controllingyour-facebook-news-feed/ (05.04.2019)

[191] A. Liptak. Sent to Prison by a Software Program's Secret Algorithms. The New York Times, 01.05.2017. Arvutivõrgus: https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-softwareprograms-secret-algorithms.html?_r=0 (05.04.2019)

toimepõhimõtted või koodi edasi jagades võimaldada kellelgi märkimisväärse investeeringu tegemiseta luua samaväärse uue programmi, kahjustades sellega nii Google-i kui ka YouTube-i konkurentsivõimet ja ärisaladuse kaitset.[192]

Eestis ei ole tehisintellektisüsteemi põhiseid kohtulahendeid, kuid ärisaladust käsitlevaid ja analüüsivad lahendeid on mitmeid. Nimelt värske uuringu alusel on Eesti kaubandusturg väike ning suur osakaal on väikeste ja keskmise suurusega ettevõtjatel[193], kelle jaoks on ärisaladuse kaitse võimalus primaarne ja ainus valik, kuivõrd ärisaladuskaitse saamiseks ei ole vaja läbida formaalseid registreerimisprotseduure. Ettevõtjate jaoks on oluline ärisaladus defineerida üheselt ja sisustada ärisaladuse määratlus, seletades töötajatele konfidentsiaalsuskohustuse ulatust ja mis täpselt ärisaladuse alla kuulub. Kohtuvaidlused on ärisaladuse kontekstis tekkinud peamiselt seeõttu, et ettevõtted ei ole suutnud üheselt ja mõistetavalt ärisaladuse ulatust määratleda, mistõttu ärisaladuse ja konfidentsiaalsuse klauslid on olnud üldistavad.[194] Kuna ärisaladuse regulatsioon on Eestis käesoleval hetkel oma olemuselt üldine ja otseselt määratlemata, kuivõrd ei sisalda konkreetset loetelu, mida oleks võimalik pidada ettevõtte ärisaladuseks, on selles kontektis vaja kohtul sisustada kaasusepõhiselt ärisaladuse mõiste ulatus.

Riigikohus enda praktikas on toonud võrdluseks Saksamaa Liidukohtu seisukohti ja pidanud analoogia korras ärisaladuse puhul samuti oluliseks, et ärisaladus, olles teada piiratud isikute ringis, peab ettevõtja saladuses hoidmise tahe olema kas dokumenteeritud või vähemalt selgelt äratuntav. Ei piisa üldsõnalisest määratlusest, vaid ärisaladuse sisu peab olema piisavalt selgelt määratletud, et kohtutel oleks võimalik tuvastada, milline on kaitset vajav ärisaladus.[195] Äriühingute jaoks tähendab see, et kui tehisintellekti algoritmi soovitakse kaitsta ärisaladusena, tuleb puudutatud isikute ringile (töötajad, ühingu juhatus) konkretiseerida algoritmi mehhanisme ja selgelt nimetada selline informatsioon konfidentsiaalseks, kusjuures ei piisa suulisest määralusest, vaid nagu kohus on öelnud, tuleks selline teave dokumenteerida. Seda

---

[192] M. Perel, N. Elkin-Koren (viide 94), lk 193

[193] A. Kelli, T. Mets, R. Rebane. Tööstusomandi kaitse ja kasutamine Eestis: majanduslik ja õiguslik perspektiiv (RITA TO). Tartu: Tartu Ülikool, 2019. Arvutivõrgus: https://www.etag.ee/wp-content/uploads/2019/01/T%C3%B6%C3%B6stusomandi-aruanne-l%C3%B5plik-11-1-2019-1.pdf (05.04.2019)

[194] A. Kelli, T. Mets, H. Pisuke, E. Vasamäe, A. Värv. Trade Secrets in the Intellectual Property Strategies of Entrepreneurs: The Estonian Experience. Review of Central and East European Law 35 (2010) 315-339, lk 337.

[195] RKTKo 09.12.2008, 3-2-1-103-08, p 20; RKTKo 11.10.2017, 2-16-1988, p 20.

aga juba vastavalt kas töölepingutes, juhatuse liikme lepingus või muus ettevõtte jaoks tähtsust omavas dokumendis. Vastavaid ärisaladust määratlevaid dokumente võiksid ettevõtted aga märkida konfidentsiaalseks arusaadava märgistusega, koostades seejuures ka ärisaladuse kaitsestrateegia.[196]

Dokumentide konfidentsiaalseks märkimine võib aga osutuda keeruliseks, kui kasutatakse kolmandate isikute poolt loodud tehisintellektisüsteeme. Põhjus seisneb asjaolus, et kui tehisintellektisüsteem on mistahes moel (litsents vms) ettevõtte kasutuses, on süsteemi toimevõime kaetud ka kellegi teise ärisaladusega. Niisiis selleks, et tagada andmesubjektile selgitus, kuidas algoritm otsustuse tegi, rikub ettevõte kolmanda isiku (juriidilise isiku) ärisaladust. Oletades, et kolmas isik, kelle poolt loodud tehisintellektisüsteemi varaliste õiguste üleandmisel, ei ole andnud süsteemi lähtekoodi, on äriühingul võimalik autoriõiguse seaduse §-st 25 tulenevalt arvutiprogrammi dekompileerimine ehk pöördprojekteerimine. Seadusest tulenevalt lubatakse pöördprojekteerimist vaid erandkorras kindlatel tingimustel ja ainult ühel eesmärgil – seda tohib teha loodava arvutiprogrammi ühilduvuse tagamiseks uuritava arvutiprogrammiga. Saadavat infot ei tohi aga üle anda kolmandatele isikutele ega kasutada olemuselt sarnase programmi arendamiseks.[197] Isikuandmete seisukohalt pole ärisaladuse avaldamine dekompileerimise teel võimalik ega ka kõige parem läbipaistvuse tagamise moodus, rikkudes oluliselt suurema isikuteringi õigusi. Lisaks algoritmide masinõppelist võimekust ja funktsionaalsust ärisaladusena kaitstes on võimalik, et ärisaladuseks peetakse ka töödeldavaid isikuandmeid.

3.2. Andmebaas ärisaladusena

Andmebaas oma olemuselt on andmete kogumik. Infotehnoloogilise loominguna on andmebaas elektrooniline teos andmete, iseseisvate teoste või muu materjali kogumik ja peab vastama teose üldistele tunnustele – peamiselt originaalsusele, sest elektrooniliste andmebaaside struktureeritus, süstematiseeritus ja kogutud sisu on selle looja loominguliste valikute tulemus ja muudab teosena andmebaasi omapäraseks. Andmebaasiteos ja selle sisu on kättesaadav

[196] A. Kelli, T. Mets, H. Pisuke, E. Vasamäe, A. Värv (viide 194), lk 325, 337

[197] M. Rosentau (viide 185), lk 765

elektrooniliste või tehniliste vahendite abil.[198] Tehisintellekti puhul on võimatu rääkida paberkandjal andmebaasist, kuivõrd intellekt ise on tehniline vahend, mille abil on võimalik teostada andmebaasipõhiseid andmetöötlustoiminguid elektrooniliselt, lihtsustades inimeste tööd, kuid vastavaid algandmeid saab tehisintellekt siiski inimestelt. Andmebaasid on vastavalt AutÕS § 4 lg 3 p-le 22 autoriõigustega kaitstavad, kuid andmebaasi mõiste ei hõlma autoriõiguse seaduse järgi selle tegemiseks ega käivitamiseks vajaminevat arvutiprogrammi.

Lisaks originaalsuse kriteeriumist lähtuvatele andmebaasiteostele, mida autoriõiguslikult kaitstakse selle sisu valiku ja korralduse unikaalsust, kaitstakse andmebaaside tegijate positsiooni seoses sisu omandamiseks ja kogumiseks tehtud finants- ja ametialaste investeeringutega seadusvastase omastamise eest, püüdes välistada kogu andmebaasi või selle olulisi osi kasutajate või konkurentide teatud toimingute eest. Niisugust õigust nimetatakse *sui generis* õiguseks, mis kaitseb investeeringuid ja isikuid, kes investeerimisriski enda peale võtavad. Investeeringud võivad seisneda finantsressursside rakendamisest, aja- ja energiakulust ning pingutustest. *Sui generis* õiguse eesmärk on anda andmebaasi tegijale õigus keelata andmebaasi sisust loata väljavõtete tegemist ja loata kasutamist.[199]

Investeeringute kaitset näeb ette AutÕS peatükk 8^1, mille § 75^3 järgi on andmebaasi tegijaks isik, kes on teinud kas laadilt, väärtuselt või suuruselt olulise investeeringu andmebaasi sisuks olevate andmete kogumiseks, omandamiseks, kontrollimiseks, süstematiseerimiseks või kättesaadavaks tegemiseks ning selleks isikuks võib olla ka äriühing. Investeeringuid tuleb aga kaitsta põhjusel, et andmebaaside loomisel võib tekkida mitmeid ühesuguseid või sarnaseid andmebaase, mis muidu autoriõiguslikule originaalsuse kriteeriumile ei vastaks ja seetõttu pole võimalik pidada teoseks. Näiteks telefoniraamatud ei täida originaalsuse kriteeriumit, kuid ometi on keegi raamatu loomiseks kulutanud enda ressursse ja teinud vastavaid pingutusi. Euroopa Kohus on leidnud, et *sui generis* õigus ei ole andmebaasi originaalsuse kaitsmiseks, vaid selleks, et hüvitada äriühingu poolt tehtud jõupingutus, mis on tehtud andmebaasis sisalduvate andmete kogumiseks, kontrollimiseks ja/või esitamiseks.[200] Sellest järeldusest võib

---

[198] *Ibid*, lk 752

[199] Euroopa Parlamendi ja nõukogu direktiiv 96/9/EÜ andmebaaside õiguskaitse kohta – ELT L 077 , 27/03/1996, preambuli p- 39-40, artikkel 7-11

[200] EK C-604/10, *Football Dataco jt*, kohtujurist P. Mengozzi ettepanek 15.12.2011, p 14. Arvutivõrgus: http://curia.europa.eu/juris/document/document.jsf?text=&docid=116724&pageIndex=0&doclang=et&mode=lst&dir=&occ=first&part=1&cid=3509406 (05.04.2019); RKTKo 06.06.2012, 3-2-1-71-12, p 12.

mõista, kui äriühing on investeeringuid teinud tehisintellekti iseõppivatesse algoritmidesse, näiteks kulutanud rahalist ressurssi töötajate väljakoolitamiseks, et arendada selline algoritm, mis kogub andmed andmebaasi, siis sellisel moel saab andmebaasi sisu *sui generis* kaitse. Andmekaitseline aspekt andmebaaside puhul tuleb mängu siis, kui andmebaasi sisuks on kliendiandmed või isikuandmed üldises tähenduses. Enne ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadust oli varasemalt kehtinud konkurentsiseaduses välja toodud näilik loetelu ärisaladuse võimalustest, mille hulka kuulusid muuhulgas oskusteavet puudutav tehniline teave ja teave klientide kohta. Hetkel kehtiv EKTÄKS lähtub ärisaladuse direktiivi regulatsioonist, mis omakorda aga TRIPS-i lepingust, mis sätestavad, et ärisaladus on selline teave, mis ei ole üldteada ega kergesti kättesaadav nende ringkondade isikutele, kes tavaliselt kõnealust laadi teabega tegelevad.

Tehisintellekti mõistes oleneb teabe kättesaadavuse kriteerium äriühingu tegevusvaldkonnast ja spetsialiseeritusest, kuid kui andmebaasi moodustavad isikuandmed, on tehisintellekti kasutava ettevõtte jaoks ärisaladuseks, tuleb ärisaladusena täpselt fikseerida, millised isikuandmed ärisaladuse kaitset vajavad. Sellise seisukoha on võtnud Riigikohus, küll mitte tehisintellekti võtmes, kuid analoogiat kasutades saab tõlgenduse tuua tehisintellekti poolt kogutud andmete konteksti. Nimelt kõnealuses vaidluses olid poolteks ettevõtted, kes pakkusid kinnisvara ostu-müügi vahendusteenust ehk maaklerteenust. Hageja nimel maaklerteenuse pakkuja ettevõtte juhatuse liige ja ainuosanik asus teise kinnisvarafirma kasuks teenuseid osutama, võttes endaga kaasa kinnisvara protfoolio, mistõttu hageja leidis, et varem avaldatud kuulutused hageja veebilehel ja erinevates veebiportaalides, mis hiljem avaldati uue äriühingu nime alt, kuulusid hageja ärisaladuse kaitse alla. Ringkonnakohtu seisukoht oli see, et arvestades hageja tegevusvaldkonda, tuleb käsitada kinnisvara müügikuulutusi ja hageja kliendiandmeid ühe tervikuna, sest kinnisvarakuulutust avaldades kasutab maakler kliendilt saadud andmeid lepingulise suhte alusel ning ilma andmete saamiseta ei ole büroo tegevus võimalik. Riigikohus leidis, et ringkonnakohtu järeldus „kuivõrd kliendiandmed on teada üksnes kinnisvarabüroole, kes pakub kliendi kinnisvara müügiks või üüriks, saab neid andmeid pidada hageja ettevõtlusega seotud spetsifiiliseks teabeks, mille avalikustamine võib hageja huve kahjustada", on lubamatult üldistav. Kohus selgitas, et ärisaladuse õigustamatu avaldamise ja kasutamise kindlakstegemiseks on vajalik võimalikult täpselt avada ärisaladuse sisu, vastasel korral võib olla takistatud vaba ettevõtlus. Teabe ärisaladuseks nimetamiseks

tuleks seega täpsustada, mida kliendiandmed ja vastav andmekogu sisaldavad ehk milliseid andmeid peetakse ärisaladuseks.[201]

Ärisaladusena isikuandmete kaitsmise võimalust lubab isikuandmete kaitse üldmääruse selgitus nr 63. Regulatsiooniga kaitstakse üksikisikute õigusi olla teadlik automatiseeritud otsuste tegemisest, nähes ette isiku võimaluse tutvuda tema töödeldavate andmetega, on andmesubjektil õigus teada eelkõige töötlemise eesmärke, võimaluse korral töötlemise ajavahemikku, isikuandmete vastuvõtjaid, isikuandmete automaatse töötlemise loogikat ja sellise töötlemise võimalikke tagajärgi. Võimaluse korral peaks vastutav töötleja saama anda andmesubjektile kaugjuurdepääsu turvalisele süsteemile tutvumaks töödeldavate andmetega, kuid samal ajal ei tohiks antud õigus kahjustada teiste isikute õigusi ega vabadusi, sealhulgas ärisaladusi.

Lugedes üldmääruse regulatiivset osa, jääb mulje, et isikuandmete kaitse ei näe üldse võimalustki, et teiste isikute õigusi ja vabadusi piiratakse ning seab esmatähtsale kohale ainult subjekti õigused. Miks antud väide omab tähtust? Üldmääruses on sõnastuses ja seega tähenduses suur erinevus, kui asetada kõrvuti eesti- ja inglisekeelsed redaktsioonid. Nimelt artiklis 15 reguleeritakse andmesubjekti õigust saada kinnitust tema suhtes töödeldavate andmete kohta ja saada vastavalt sisulist teavet automatiseeritud otsuste tegemisel kasutatava loogika kohta[202] ja vastutav töötleja esitab töödeldavate isikuandmete koopia[203]. Artiklis 20 sätestatakse õigusnormid andmete ülekandmiseks ühelt vastutavalt töötlejalt teisele - isikul on õigus saada teda puudutavaid isikuandmeid, mida ta on vastutavale töötlejale esitanud masinloetavalt ja struktureeritud kujul ning edastada need andmed teisele vastutavale töötlejale.

Mõlema artikli 4. lõiked teevad tagasiviite: artikli 15 lg 4 ütleb, et lõikes 3 sätestatud koopia tegemise õigus „ei kahjusta teiste isikute õigusi ja vabadusi"; artikli 20 lg 4, et lõikes 1 sätestatud andmete saamise ja ülekandmise õigus „ei kahjusta teiste isikute õigusi ja vabadusi". Kuivõrd eestikeelne redaktsioon kinnitab, et nimetatud õigused teiste isikute õigusi ja vabadusi ei kahjusta, tekib arusaam, et seadusandjad on juba ette näinud teiste isikute õiguste ja vabaduste mittekahjustumist andmekaitselistest reeglitest kinnipidamisel ning määranud sõnaselgelt must-valgena, et see nii on. Võrreldes eestikeelset redaktsiooni inglisekeelsega,

[201] RKTKo 10.05.2017, 3-2-1-36-17, p 13

[202] GDPR, artikkel 15 lg 1 (h)

[203] GDPR, artikkel 15 lg 3

tekib oluline tähenduslik erinevus, sest inglisekeelset üldmäärust lugedes sätestavad lõiked 4 klausli: *shall not adversely affect the rights and freedoms of others*, mis eesti keelde tõlgituna peaks tähendama, et vastavad õigused, millele on artiklite lõigetes 4 viidatud, ei tohi kahjustada teiste isikute õigusi ja vabadusi. Kõrvutades ettevõtlusvabadusega seonduvat ärisaladuse kaitset andmekaitselises määratluses, selgub, et andmesubjekti andmetega tutvumise ja koopiate tegemise võimalus ei tohiks üldmääruse järgi kahjustada ettevõtja ärisaladust.

Ärisaladuse kaitse direktiivi kohaselt tuleb järgida põhiõigusi ja võtta arvesse eelkõige hartaga tunnustatud põhimõtteid, eriti õigust era- ja perekonnaelu puutumatusele, õigust isikuandmete kaitsele, sõna- ja teabevabadust ning ettevõtlusvabadust. On oluline, et järgitaks ka era- ja perekonnaelu puutumatus ja andmekaitse õigusi, kui ärisaladuse omaja töötleb isikuandmeid ärisaladuse kaitseks võetavate meetmetega.[204] Sisuliselt peaks direktiivi selgitust tõlgendama selliselt, et kui ärisaladusena kaitstakse isikuandmeid, tuleks kohaldada samaaegselt isikuandmete kaitse regulatsiooni. Direktiivi artikkel 13 lg 1 (h) alusel on liikmesriikide kohtutel kohustus ärisaladusega seonduvate nõuete hindamisel arvestada ka põhiõiguste kaitset. Viidates tagasi isikuandmete regulatsioonile, annab üldmääruse artikkel 23 liikmesriikidele kaalutlusruumi seadusandlike meedetega piirata artiklites 12–22 ja artiklis 34 ja 5 sätestatud kohustuste ja õiguste ulatust, kui selline piirang siiski austab põhiõiguste ja -vabaduste olemust. Samuti peavad piiratavate õiguste ja kohustuste ulatus olema demokraatlikus ühiskonnas vajalik ja proportsionaalne, tagamaks teiste isikute õiguste ja vabaduste kaitse.[205]

Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus isikuandmete kaitse osas proportsionaalset meedet ei sätesta, kuid esitleb §-s 7 nõudeõigusi, kui ärisaladust kasutatakse ebaseaduslikult, kusjuures nõudeid võib esitada, kui need on proportsionaalsed, arvestades muu hulgas kolmanda isiku õigustatud huve[206]. Nimetatud seaduse seletuskirjas on selgitatud, et seadusandja ei näe vajadust ärisaladuse direktiivi artiklit 13 lõike 1 punkti h eraldiseisvalt riigisisesesse õigusesse üle tuua, sest põhiõiguste kaitse ja kohtuvõimu kohustus neid järgida tuleneb põhiseaduse §-st 14.[207]

---

[204] Ärisaladuse direktiiv, selgitused 34-35

[205] GDPR, artikkel 23 lg 1 (i)

[206] EKTÄKS § 7 lg 2 p 6

[207] Seletuskiri ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse eelnõu juurde 678 SE. 22.08.2018, lk 7. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9b6f21b8-db1c-436d-a045-326913d80d22 (05.04.2019)

Kui mõlema valdkonna regulatsioonid, millest ühelt poolt on füüsiliste isikute põhiõigus isikuandmete kaitsele ja teiselt poolt on juriidiliste isikute põhiõigus ettevõtlusvabadusega kaasnev ärisaladuse kaitse, on omavahel vastuolus, tuleb leida tasakaal. Kummagi valdkonna õigusaktid ei sätesta kummagi õigusakti tähtsamat osakaalu, vaid viitavad teineteisele, mistõttu tarvis kohtutel kaasuspõhiselt välja selgitada rikkumise ulatust hinnates, kumma poole põhiõigused vajavad suuremat kaitset. Tehisintellekti valdkonna puhul, kui ühest küljest on ärisaladusega kaitstud algoritmid ning teisest küljest andmbaasi sisu nii *sui generis* õigusega ja ärisaladusega, seisneb probleemi olemus läbipaistvuses. Ärisaladus läbipaistvust ei võimalda, isikuandmete kaitse läbipaistvuseks seevastu kohustab. GDPR inglisekeelse redaktsiooni selgituse punktile 63 vastavalt ei tohiks andmesubjektile antud juurdepääsu õigus rikkuda ärisaladuse kaitset, kuid lõpptulemusena ei tohiks ettevõte täielikult keelduda igasuguse informatsiooni jagamisest[208], vaid talle on antud võimalus täpsustada andmesubjektilt, milliste töötlemistoimingutega tema taotlus seotud on. Automatiseeritud andmetöötluse puhul, kui kasutatakse masinõppivaid algoritme, peab ettevõtja suutma määratleda, millise kategooria ja spetsiifikaga andmed tema andmebaasis on ärisaladusena kaitset vajavad ja milliseid andmeid on tal võimalik isikule jagada. Ärisaladust kaitsvad õigusnormid, mis toetavad juriidiliste isikute ettevõtlusvabadust, ei tohiks kahjustada andmesubjektide õigusi ja vastupidi, mistõttu äriühing ei tohiks täielikult peituda ärisaladuse kaitseloori taha, vaid informatiivselt ja kokkuvõtlikult selgitama töödeldavaid andmeid vähemalt selles osas, mis ärisaladuse hulka ei kuulu.[209] Suurkorporatsioonid nagu Facebook[210], Google ning ka teised mistahes suurusega äriühingud, mis tehisintellekti algoritmilist loogikat kaitsevad ärisaladuse mehhanismiga, on siiski kohustatud füüsilisi isikuid, kes on enda positsioonilt nõrgemas seisus, teavitama töötlusprotsessi kuuluvatest andmetest kasvõi üldistatult ja mitte täielikult keelduma andmete salajasuse tõttu neid avaldamast.

Infoühiskonnas, kus suurehulgaliste andmete töötlemiseks kasutatakse tehisintellektisüsteeme, langevad juriidiliste isikute majandustegevusega seotud andmed peamiselt kokku kliendi- ja

---

[208] GDPR, selgitus 63 „However, the result of those considerations should not be a refusal to provide all information to the data subject.”

[209] P. Hustinx. Opinion of the European Data Protection Supervisor. Brüssel, 12.03.2014, lk 5. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf (06.04.2019)

[210] Facebook keeldus päringule vastamisel igasugusest informatsiooni jagamisest, peitudes intellektuaalomandi ja ärisaladuse õiguskaitse taha, kuid viimase aja õiguskorra muudatustega just samalaadseid olukordi soovitaksegi vältida. Vt: http://www.europe-v-facebook.org/FB_E-Mails_28_9_11.pdf (06.04.2019)

tarbijaandmetega, mille kaubandusliku väärtuse olemasolus pole vaidlustki[211], võiksid andmesubjekti nõusolekul antud andmed jäädagi ärisaladuseks ja subjektide jaoks läbipaistmatuks. Käesoleva töö autor ei pea siinkohal silmas, et kõik füüsilise isiku nõusolekul saadavad andmed lepingu täitmiseks või teenuse pakkumiseks peaksid jääma saladuseks, aga äriühingul peaks siiski jääma võimalus takistada juurdepääs ja salastada andmed, mida konkreetselt kasutatakse ettevõtte majandustegevusega. Nõustudes siinjuures kohtute praktikaga, peaksid majandustegevuses toimivad isikud, kes ärisaladusena kaitsevad kasutatava tehisintellektisüsteemi algoritmilist toimimisloogikat, mõistma algoritmi käitumist, teadmaks, millist liiki andmeid algoritmide kõrval andmebaasides kaitsta.

Ärisaladuse sisu ja töödeldavate andmete sisu mõistmine on tähtis, kui kehtiv õigus võimaldab andmete ülekandmist.[212] Olukorras, kus tehisintellekti algoritmid koguvad andmeid automatiseeritult ning ettevõtja on investeerinud algoritmi arendamisele, siis lisaks andmesubjektilt saadud andmetele, teeb algoritm olemasolevate andmete põhjal ka muid kokkuvõtteid, järeldusi, et täiustada end otsuste tegemisel ja teiseks olla ettevõttel vahendiks äriliste eesmärki täitmisel, mistõttu lubades isikul kanda andmed üle teisele vastutavale töötlejale, peaks andmete ülekandmise õigus piirdumagi ainult nende andmetega, mille töötlemise kohta on andmesubjekt nõusoleku andnud. Siinkohal pöörab autor tähelepanu asjaolule, et kui ettevõtte ärisaladusega kaitstud algoritm jäljendab intellektuaalset tegevust ja integreerib iseõppimise tulemusena teatavad andmed andmebaasi, siis selliste andmete ülekandmine elektrooniliste vahendite abil võib avaldada endise vastutava töötleja ärisaladuse – ehk konfidentsiaalse teabe, milliseid andmeid algoritm otsustuste tegemisel kasutab ja millise ärilise eesmärgiga.

Valikuliselt andmetele juurdepääsu keelamine võib küll tekitada klientide ja ettevõtete vahelise asümmeetria, mis võib tunduda ebaproportsionaalne, kuid võttes arvesse mõlema poole põhiõigusi, on selline ärisaladuslik kaitse teatavatele andmetele siiski vajalik, austamaks majanduslikku vabadust innovatsiooni levikuks ja austamaks ettevõtete intellektuaalset omandit. Sarnaselt on ka klientidel või tarbijatel võimalik otsustada, milliseid andmeid nad äriühingule avaldamata jätavad. Andmetel on vastavalt isikuteringile oma väärtus, mistõttu

[211] G. Malgieri. Trade Secrets v Personal Data: a possible solution for balancing rights. International Data Privacy Law, 2016, Vol. 6, No. 2, lk 106. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002685 (06.04.2019)

[212] GDPR, artikkel 20

kaitstakse andmeid erinevatel põhjustel ja erinevates kontekstides, seepärast tuleks tehisintellekti juures ärisaladuse regulatsioonis võtta aluseks kontseptsiooniline lähenemisviis, mille alusel eraldatakse isiku jaoks tähtsust omavad andmeliigid majanduslikust kontekstist ilma ettevõtte huve kahjustamata.[213]

On selge, et andmebaasid, mida investeeringuna kaitstakse, omavad ärsialaduslikku kaitset, kui neil on kaubanduslik väärtus. Andmete kaubanduslik väärtus aga peamiselt sõltub investeeringute suurusest, mis on andmete kogumiseks tehtud, andmete salastatusest ja sellest, millist hinda ollakse nõus maksma nende andmete saamise eest[214] (nt andmevahendajalt andmete ostmise korral). Sellest tulenevalt saavad kliendiandmed kaitstuks ärisaladusena, kui need moodustavad terviku ja on oma struktuurilt mahukad. Seepärast ainult ühe inimese andmed, mida on võimalik tehisintellektisüsteemist väljavõttena isikule võimaldada, ei oma ärisaladuse mõttes otsest kaubanduslikku väärtust ega pruugi otseselt mõjutada ettevõtte poolt kasutatava tehisintellekti intellektuaalset panust[215], kuid võivad siiski mingil kujul anda aimu algoritmide kasutatavast loogikast. Selleks, et ettevõttel oleks aga võimalik ärisaladuse kaitsele tugineda, peaks ettevõte väga täpselt määratlema, millist kasutatavat teavet (masinõppelise programmi puhul kõikvõimalikud töötlusprotsessid ja isikuandmete kontekstis loetelu, milliseid andmeid kasutatakse) peab ta enda jaoks ärisaladuseks, koostades vastava saladuse kaitse strateegia, mis tagaks ärisaladuse jaoks parema ülevaate ja kaitsemehhanismi.

[213] G. Malgieri (viide 211), lk 115

[214] M. Maarand. Ärisaladuse olemus ja tsiviilõiguslik kaitse lepinguvälistes võlasuhetes. Tartu Ülikool, Tallinn 2014, lk 18-19. Arvutivõrgus: http://dspace.ut.ee/handle/10062/42984 (07.04.2019)

[215] G. Malgieri (viide 211), lk 115

KOKKUVÕTE

Tehisintellekt on masinõppeline algoritm, millel on võime jäljendada inimese intelligentsust ja mida kasutatakse igapäeva toimetuste hõlbustamiseks. Algoritm suudab õppida äärmiselt suurest hulgast andmetest, mille hulka kuuluvad samuti isikuandmed, ning võtta iseseisvalt vastu automatiseeritud otsuseid, mis võivad inimesi õiguslikult ja märkimisväärselt mõjutada.

Käesoleva magistritöö eesmärgiks oli selgeks teha, kas tehisintellekti poolt isikuandmete töötlemisel on võimalik kehtivate õigusnormide alusel tagada isikutele täielik läbipaistvus ja selgus algoritmide iseõppimise käigus tehtavatele automatiseeritud otsuste suhtes, kui algoritme kasutaval vastutaval töötlejal on tehisintellekti toimimismehhanismid ja töödeldavad andmed kaitstud ärisaladusena. Eesmärgi täitmiseks seadis autor hüpoteesi, et isikuandmete kaitse regulatsioon piirab eraõiguslike juriidiliste isikute põhivabadust tegeleda ettevõtlusega ja läbipaistvuse tagamine ärisaladuse konfidentsiaalsusnõude aspektis takistab konkurentsvõimekust, mistõttu täielikku läbipaistvust isikuandmete töötlemisel ei ole võimalik saavutada.

Andmekaitseline regulatsioon lähtub fundamentaalsest andmete töötlemise põhimõttest – läbipaistvus, mille järgi peavad andmetöötlejad võimaldama subjektile automatiseeritud otsuste puhul sisulist teavet algoritmi poolt kasutatava loogika kohta. Läbipaistvuse põhimõte eedab, et andmesubjektidel on õigus saada nimetatud loogika kohta selgitusi lihtsas ja selges keeles ning arusaadavalt. Tehisintellektid käituvad tehnilisel tasandil musta kastina, mis tähendab, et oma süsteemi keerukuse ja iseõppimise oskuse tõttu, ei ole võimalik algoritmide töötlemistoiminguid ja kasutatavat loogikat andmesubjektile selgitada. Peamiselt seetõttu, et algoritmide otsustetegemise protsessid on keerulised tehisintellekisüsteemi programmeerijatelegi ning selgituskohustust ei ole võimalik täita, kui selgitused sisaldavad tehnilist ja matemaatilist teavet, mis ei ole tehniliste teadmisteta andmesubjekti jaoks mõistetav.

Tehisintellekti läbipaistvuse tagamist piirab õiguslik „must kast", mille puhul tuleb ületada isikuandmete kaitse ja ärisaladuse regulatsiooni omavaheline vastuolu, kus ühelt poolt läbipaistvuse kriteerium ning teiselt poolt konfidentsiaalsuse kriteerium. Tagamaks läbipaistev andmetöötlus, eriti algoritmide poolt automatiseeritud otsustes kasutatavat loogikat sisulise teabega selgitamisel, tuleb avada must kast tehniliselt, et mõistmaks alustuseks, kuidas ta toimingute tegemise protsessis mõtleb ja milliseid andmeid isikute kohta töötleb. Ärisaladuse

regulatsioon seevastu sätestab, et ärisaladusena on võimalik kaitsta arvutitarkvara töötlemisprotsesside tööpõhimõtteid ja töödeldavaid andmeid, kui selline teave, mida ettevõtja ärisaladusena kaitseb, ei ole kogumis või üksikute osade paigutuses üldteada ega samas valdkonnas tegutsejatele kergesti kättesaadav. Kui algoritmilise otsustuse põhiprotsessid on ärisaladusena kaitstavad ja masinõppivad algoritmid enda täiustamise funktsioonist tulenevalt ei ole samuti kergesti jälgitavad, siis nimetatud kriteerium on ärisaladuse mõttes täidetud, kuid ettevõte ise peab aga omama aimu nendest protsessidest ja töödeldavatest andmetest. Eesti kohtupraktikas on siiani ärisaladust käsitlevate vaidluste lahendamisel võetud seisukoht, et teavet on võimalik kaitsta siis, kui on teada, milline on ärisaladuse kaitset vajava teabe sisu. See tähendab ettevõtjate jaoks, et ärisaladuse määratlus tuleb ettevõtte siseselt selgeks teha ehk avada musta kasti protsessid ja teada täpselt, kuidas tehisintellekt toimib, milliseid andmeid kasutab ja milliseid järeldusi suudab teha. Tehisintellekti puhul on seda praktikas äärmiselt keeruline saavutada, kuid teatavaid põhimõtteid töötlemistoimigute teostamisel peaks ettevõtja aga siiski suutma formuleerida ärisaladuse kaitsmiseks. Ärisaladuse olemus tuleks ettevõtetel dokumenteerida, vältimaks ettevõtetesiseseid arusaamatusi ärisaladuse olemuse erinevatest tõlgendustest ning kaitsmaks konfidentsiaalselt informatsiooni selle avalikustamise eest. Seejuures on oluline, et ettevõte tehtud investeeringuid kaitseks stateegiliselt ja koostaks üksikasjaliku ärisaladust sisaldavad aspektid.

Ärisaladusena kaitstaval teabel peab olema kaubanduslik väärtus, mis tekib eelkõige teabe salajasuse kriteeriumist ning väärtus on mõõdetav tehtud investeeringute suuruse ja teavet omandada soovija poolt pakutava hinnaga. Tehisintellekti algoritmide ja protsessitoimingute osas pole vaidlustki, et neil on ärisaladuse kaitsest tulenevalt ka kaubanduslik väärtus, kuivõrd tehisintellekti arendamisel osaleb palju inimesi ja ettevõte on teinud suuri investeeringuid tehisintellekti kasutuselevõtmiseks. Andmetel on erinevate isikuterühmade jaoks erinev väärtus – kelle jaoks majanduslik ja äriline rahas mõõdetav väärtus, kelle jaoks privaatsusaspektiline väärtus. Andmetöötluses kasutatavate isikuandmete ja muude andmete puhul on andmetel kaubanduslik väärtus kogumis, sest üksikult kogumist eraldatult andmeid ei osteta, vaid ostetakse tervikliku andmebaasi sisuna. Kui ettevõte leiab, et tagades ühele isikule tehisintellekti algoritmi poolt kogutud andmete seast andmebaasist väljavõte, võib üksikisik saada aimu ettevõtte ärisaladusest, peab ettevõte olema suuteline väljavõtte tegemisel isikult üle täpsustama, milliseid andmeid ta täpselt soovib. Vastasel juhul võib ettevõte kaotada andmete väljavõtte võimaldamisel ärisaladuse kaitse, kui just need andmesubjekti poolt saadavad andmed kuuluvad ettevõtte majandusliku kasumlikkuse huvisse.

Käesolevat tööd kirjutades selgus asjaolu, et isikuandmete ja ärisaladuse kaitse regulatsioonid on koostatud isikute põhiõigusi arvestades, kuid ei anna regulatsioonide mõttes täpsustust, millisel neist on kõrgem osakaal vaidluste tekkimise korral. Hetkel kehtiv õigus annab võimaluse takistused ületada kohtutel, kuid kohtupraktika järgi tundub, et ärisaladuse üldsõnalise regulatsiooni tõttu on andmesubjektide õigus läbipaistvaks andmetöötluseks tagatud paremini. Seetõttu teeb autor ettepaneku konkretiseerida ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadust ärisaladuse ja isikuandmete kaitse võtmes. Samuti tuleks ettevõtjatele nende ettevõtlusvabaduse rakendamiseks määrata parema ärisaladuse kaitse tagamiseks seaduse alusel kohustus koostada ärisaladuse kaitsestrateegia, kuivõrd praeguses õiguskorras selline kohustus puudub.

INTERACTION BETWEEN TRADE SECRET AND DATA PROTECTION REGULATION IN TRANSPARENCY OF ARTIFICIAL INTELLIGENCE

Summary

Nowadays, technology is developing at a rapid pace, and more and more people rely on smart technological means in everyday life. The biggest development in the 21st century has been the deployment of artificial intelligence (AI) in many fields such as medicine, art, industry, law and much more. It is difficult to unambiguously define artificial intelligence, because the definitions are mainly based on the nature of the task assigned to the artificial intelligence.

Artificial intelligence is a branch of computer science and technology that aims to develop theories, methods, applications, and algorithms that mimic and expand human intelligence. Mainly artificial intelligence refers to a self-learning algorithm trained with machine learning technology. This allows system to learn from vast amount of data, including personal data, and to independently adopt automated decisions that can affect people legally and significantly. AI brings a lot of risks, so it is important that the code of ethics and the relevant legislation are developed. In 2018 European Union Member States signed Declaration of cooperation on Artificial Intelligence and the Ministry of Economic Affairs and Communications of Republic of Estonia called up a group of experts to prepare a bill to allow the use of AI[216].

Large-scale data processing with the use of artificial intelligence threatens people's fundamental rights, in particular the right to privacy, which is why The European Parliament and The Council have adopted regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation – hereinafter GDPR). Data protection regulation is based on the fundamental principle of processing - transparency, by which data controllers must provide the data subject substantive information about the logic used in the algorithmically automated decisions.

[216] See the Government Office's press release: https://www.riigikantselei.ee/en/news/estonia-will-have-artificial-intelligence-strategy (01.02.2019)

In the light of the bill of AI being prepared by the Estonian Republic's Ministry of Economic Affairs and Communications and GDPR entered into force, the purpose of this thesis is to determine whether the processing of personal data by an artificial intelligence allows, under applicable law, full transparency and clarity for individuals in the automated decisions made during the self-learning of the algorithms, if the data controller using the algorithms has the mechanisms of artificial intelligence and processed data protected as trade secrets.

To achieve this goal, the author hypothesized that the regulation of personal data protection limits the fundamental freedom of private legal entities to engage in business and that transparency in the aspects of confidentiality requirement of trade secrets hinders the competitiveness, therefore full transparency in the processing of personal data cannot be achieved. The thesis is based on an analytical method of research. There is also a systemic-qualitative method in use, as the author discusses the issues related to the hypothesis, the necessary adaptations of the current law and makes corresponding proposals.

The thesis is divided into three chapters to achieve the objective. In the first chapter the author analyzes the nature of artificial intelligence and machine-learning, how are these related to the processing of data. Artificial intelligence's technique machine learning enables private data controllers to analyse big data in order to make decisions in an automated way, so artificial intellgence is using as much data as possible. The fact is that the more accurate an algorithm, the less transparent it is and makes the rationale behind the automated decisions difficult to access. Technically this has been called as black box and relates to lack of transparency.

In the second chapter, the author analyzes how the principle of transparency is provided in data regulation. The principle of transparency in data regulation means that the logic behind an automated decision is explained to the data subject in an understandable and simple language, however in the context of the black box it is quite difficult to provide the data subject a meaningul information in terms which might be understandable for the subject. In author's opinion the transparency principle involves the data subject's right to an explanation, although the ragulation does not give the exact obligation in the sense of explanation rather points out the right for information.

Third chapter analyzes the artificial intellegence as legal black box whereas the logic behind the automated decisions can be protected by trade secret mechanism. Trade secret regulation is

determined in Directive 2016/943 of The European Parliament and of the Council and in Estonian legislation Restriction of Unfair Competition and Protection of Business Secrets Act.[217] Both regulations state that in order to get the protection under trade secrecy following requirements must be met: it is secret in the sense that it is not, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question; it has commercial value because of its secrecy; the person lawfully in control of the information takes reasonable steps to keep it secret. So if data controller provides meaningful information about the logic used in algoritmic processes, the information loses its secrecy. This refers to the legal black box of AI. In the practice of Estonian courts, in order to protect any information as trade secret, it is important to know the content of the trade secret, so the content of trade secret must be clearly defined within the company[218].

Keeping all this in mind, the author finded out that in current legislation it is not clear whether fundamental rights of private companies or of data subjects need stronger protection in the context of trade secret and data processing. However, if the companies want to protect their trade secret in which they have made investments, they still need to understand the knowledge and processes behind algorithmic decisions, documenting this knowledge in company's internal documents.

In conclusion the author suggests that to protect private companies' investments and to keep the aspects of trade secret a secret, the companies as well the legislator of Estonian Republic needs to regulate trade secret protection strategy as mandatory obligation for companies. Therefore the author confirms the hypothesis - full transparency under the current regulation cannot be guaranteed.

[217] Restriction of Unfair Competition and Protection of Business Secrets Act is found in here: https://www.riigiteataja.ee/en/eli/520122018013/consolide (07.04.2019)

[218] RKTKo 11.10.2017, 2-16-1988. Decisions of the Estonian Supreme Court are published on the web page of the Supreme Court www.riigikohus.ee.

KASUTATUD LÜHENDID

AutÕS – Autoriõiguse seadus

EK – Euroopa Kohus

EKTÄKS – Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus

GDPR – Euroopa Parlamendi ja Nõukogu määrus 2016/679

IKS – Isikuandmete kaitse seadus

PS – Eesti Vabariigi põhiseadus

RKTK – Riigikohtu tsiviilkolleegium

TRIPS-i leping – Intellektuaalomandi õiguste kaubandusaspektide leping

KASUTATUD MATERJALID

Kirjandus

1. AI Composer Creates Music for Films and Games. – NVIDIA Developer, 16.03.2017. Arvutivõrgus: https://news.developer.nvidia.com/ai-composer-creates-music-for-films-and-games/ (01.03.2019)
2. A. D. Selbst, J. Powles. Meaningful information and the right to explanation. International Data Privacy Law, 2017, Vol. 7, No. 4. Arvutivõrgus: https://doi.org/10.1093/idpl/ipx022 (20.03.2019)
3. AISB. The Society for the Study of the Artificial Intelligence and Simulation of Behaviour. Loebner Prize. Arvutivõrgus: https://www.aisb.org.uk/events/loebner-prize (02.02.2019)
4. A. Kelli, T. Mets, H. Pisuke, E. Vasamäe, A. Värv. Trade Secrets in the Intellectual Property Strategies of Entrepreneurs: The Estonian Experience. Review of Central and East European Law 35 (2010) 315-339
5. A. Kelli, T. Mets, R. Rebane. Tööstusomandi kaitse ja kasutamine Eestis: majanduslik ja õiguslik perspektiiv (RITA TO). Tartu: Tartu Ülikool, 2019. Arvutivõrgus: https://www.etag.ee/wp-content/uploads/2019/01/T%C3%B6%C3%B6stusomandi-aruanne-l%C3%B5plik-11-1-2019-1.pdf (05.04.2019)
6. A. Liptak. Sent to Prison by a Software Program's Secret Algorithms. The New York Times, 01.05.2017. Arvutivõrgus: https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-softwareprograms-secret-algorithms.html?_r=0 (05.04.2019)
7. A. Metzger. Data as Counter-Performance: What Rights and Duties do Parties Have? JIPITEC 2 para 1. 2017. Arvutivõrgus: https://www.jipitec.eu/issues/jipitec-8-1-2017/4528/jipitec_8_1_2017_metzger_data%20as%20counter-performance.pdf (01.03.2019)
8. A. M. Turing. Computing Machinery and Intelligence. - Mind 49, 1950. Arvutivõrgus: https://www.csee.umbc.edu/courses/471/papers/turing.pdf (02.02.2019)
9. Article 29 Data Protection Working Party (Artikkel 29 töörühm). Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. 06.02.2018. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 (18.03.2019)
10. Article 29 Data Protection Working Party (Artikkel 29 töörühm). Guidelines on transparency under Regulation 2016/679. 11.04.2018. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227 (19.03.2019)

11. Apple Siri. https://www.apple.com/ios/siri/ (01.03.2019)
12. B. Custers. Data Dilemmas in the Information Society Introduction and Overview. Raamatust Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases. 1. peatükk, vol 3. Springer 2013, lk-d 3-26. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)
13. B. Lundqvist. Big Data, Open Data, Privacy Regulations, Intellectual Property and Competition Law in an Internet of Things World. Faculty of Law, University of Stockholm. Research Paper No. 1/2016. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2891484 (17.03.2019)
14. B. Marr. The Key Definitions Of Artificial Intelligence (AI) That Explain Its Importance. 14.02.2018. Arvutivõrgus: https://www.forbes.com/sites/bernardmarr/2018/02/14/the-key-definitions-of-artificial-intelligence-ai-that-explain-its-importance/ (02.02.2019)
15. B. Marr. Where Can You Buy Big Data? Here Are The Biggest Consumer Data Brokers. Forbes, 2017. Arvutivõrgus: https://www.forbes.com/sites/bernardmarr/2017/09/07/where-can-you-buy-big-data-here-are-the-biggest-consumer-data-brokers/#5ba8f18c6c27 (10.02.2019)
16. C. Kuner, D. J. B. Svantesson, F. H. Cate, O. Lynskey, C. Millard. Machine learning with personal data: is data protection law smart enough to meet the challenge? International Data Privacy Law, 2017, Vol. 7, No. 1. Arvutivõrgus: https://academic.oup.com/idpl/article/7/1/1/3782694 (18.03.2019)
17. CLEVERISM. Artificial Intelligence: A Complete Guide. 2015. Arvutivõrgus: https://www.cleverism.com/artificial-intelligence-completeguide/ (02.02.2019)
18. C. Quackenbush, A Painting Made by Artificial Intelligence Has Been Sold at Auction for $432,500. 26.10.2018. TIME USA, LLC. Arvutivõrgus: http://time.com/5435683/artificial-intelligence-painting-christies/ (01.03.2019)
19. Deloitte. AI and You: Perceptions of Artificial Intelligence from the EMEA financial services industry. 2017. Arvutivõrgus: https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/technology/deloitte-cn-tech-ai-and-you-en-170801.pdf (02.02.2019)
20. D. Castelvecchi. Can we open the black box of AI?. Nature, 2016. Arvutivõrgus: https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731 (14.03.2019)

21. D. Kamarinou, C. Millard, J. Singh. Machine Learning with Personal Data. Queen Mary University of London, School of Law Legal Studies Research Paper 247/2016. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2865811 (25.03.2019)
22. J. Laffranque, C. Ginter, R. Laffranque, Ü.Madise, L. Mälksoo, J. Põld, A. Tupits. Põhiseaduse täiendamise seaduse kommentaarid. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura 2017. Arvutivõrgus: https://www.pohiseadus.ee/index.php?sid=3&p=2 (17.03.2019)
23. Euroopa Andmekaitseinspektori soovitused ELi andmekaitsereformi võimaluste kohta. ELT C 301/1, 12.09.2015. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52015XX0912(01)&qid=1554705163152 (17.03.2019)
24. E. Brynjolfsson, A. McAfee. Artificial Intelligence, For Real. Harvard Business Review: The Big Idea. 2017. Arvutivõrgus: http://asiandatascience.com/wp-content/uploads/2017/12/Big-Idea_Artificial-Intelligence-For-Real_The-AI-World-Confernece-Expo-Decembe-11_13-2017.pdf (08.02.2019)
25. Euroopa Komisjon. Commission Staff Working Document. Impact Assessment. Accompanying the document proposal for a Directive of the European Parliament and of the Council on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure. Brussels, 28.11.2013. SWD(2013) 471 final. Arvutivõrgus: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2013:0471:FIN:EN:PDF (04.04.2019)
26. Euroopa Komisjon. Komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele: Tehisintellekt Euroopa huvides. Brüssel, 2018. Arvutivõrgus: http://ec.europa.eu/transparency/regdoc/rep/1/2018/ET/COM-2018-237-F1-ET-MAIN-PART-1.PDF (05.02.2019)
27. Euroopa Komisjon. EU Member States sign up to cooperate on Artificial Intelligence. 10.04.2018. Arvutivõrgus: https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence (02.02.2019)
28. Euroopa Komisjon. Kirjuta selgelt. EU publications, 16.03.2011. Arvutivõrgus: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5/language-et (19.03.2019)
29. Euroopa Majandus- ja Sotsiaalkomitee arvamus teemal „Komisjoni teatis Euroopa Parlamendile, Euroopa Ülemkogule, nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele

ning Regioonide Komiteele „Tehisintellekt Euroopa huvides““ (COM(2018) 237 final). ELT C 440/51. 06.12.2018. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52018AE2369 (16.03.2019)

30. Euroopa Parlament. Tööstuse, teadusuuringute ja energeetikakomisjon. Raport tehisintellekti ja robootika valdkonna Euroopa tervikliku tööstuspoliitika kohta (2018/2088(INI)). 30.01.2019. Arvutivõrgus: http://www.europarl.europa.eu/doceo/document/A-8-2019-0019_ET.html (16.03.2019)
31. F. Anifowose, A. Khoukhi, A. Abdulraheem. Investigating the effect of training–testing data stratification on the performance of soft computing techniques: an experimental study. 2017. Journal of Experimental & Theoretical Artificial Intelligence. VOL. 29, NO. 3. Arvutivõrgus: https://doi.org/10.1080/0952813X.2016.1198936 (11.02.2019)
32. F. Pasquale. The Black Box Society: The Secret Algorithms That Control Money and Information. Harvard University Press, 2015. Arvutivõrgus http://www.hup.harvard.edu/catalog.php?isbn=9780674368279 (06.03.2019)
33. Gartner IT Glossary. Big Data. Arvutivõrgus: https://www.gartner.com/it-glossary/big-data (17.02.2019)
34. G. Malgieri. Trade Secrets v Personal Data: a possible solution for balancing rights. International Data Privacy Law, 2016, Vol. 6, No. 2. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002685 (06.04.2019)
35. G. Noto La Diega. Against the Dehumanisation of Decision-Making. 2018. Arvutivõrgus: https://www.jipitec.eu/issues/jipitec-9-1-2018/4677/JIPITEC_9_1_2018_3-34 (14.03.2019)
36. H. Hodson. The secret system controlling your Facebook News Feed. New Scientist, 30.07.2014. Arvutivõrgus: https://www.newscientist.com/article/mg22329804-200-the-secret-system-controllingyour-facebook-news-feed/ (05.04.2019)
37. Information Commisoner's Office. Big data, artificial intelligence, machine learning and data protection. 04.09.2017. Arvutivõrgus: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (17.02.2019)
38. Information Commisioner's Office. Feedback request - profiling and automated decision-making. 28.04.2017. Arvutivõrgus: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/feedback-request-profiling-and-automated-decision-making/ (18.03.2019)
39. J. A. Kroll, J. Huey, S. Barocas, E. W. Felten, J. R. Reidenberg, D. G. Robinson, H. Yu. Accountable Algorithms. University of Pennsylvania Law Review, Iss. 3, 2017, Vol. 165:

633. Arvutivõrgus: https://scholarship.law.upenn.edu/penn_law_review/vol165/iss3/3/ (25.03.2019)

40. J. Maring. Samsung Bixby: Everything you need to know! Android Central, 22.02.2019 Arvutivõrgus: https://www.androidcentral.com/bixby (01.03.2019)
41. J. York. Getting banned from Facebook can have unexpected and professionally devastating consequences. Quartz Media, 31.03.2016. Arvutivõrgus: https://qz.com/651001/getting-banned-from-facebook-can-have-unexpected-and-professionally-devastating-consequences/ (19.03.2019)
42. L. Deng. Artificial Intelligence in the Rising Wave of Deep Learning - The historical path and future outlook. IEEE Signal Processing Magazine. 2018. Arvutivõrgus: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8253597 (02.02.2019)
43. L. Edwards, M. Veale. Slave to the algorithm? Why a 'right to an explanation' is probably not the remedy you are looking for. Duke Law & Technology Review, 2017, Vol. 16, no. 1. Arvutivõrgus: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1315&context=dltr (01.04.2019)
44. M. Aim. Tehisintellekti kasutamispraktikad ja arenguperspektiivid Eesti finantssektori näitel. Tartu: TÜ Majandusteaduskond 2018. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/61160/aim_mariel.pdf?sequence=1&isAllowed=y (02.02.2019)
45. M. C. Elish. Moral Crumple Zones Cautionary Tales in Human-Robot Interaction. Data & Society Research Institute, 03.04.2016. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757236 (19.03.3019)
46. M. Koit, T. Roosmaa. Tehisintellekt. Tartu: TÜ Arvutiteaduse instituut 2011. Arvutivõrgus: https://dspace.ut.ee/bitstream/handle/10062/28296/tehisintellekt.pdf?seq (02.02.2019)
47. M. Krenchel, C. Madsbjerg. Your Big Data Is Worthless If You Don't Bring It Into The Real World. WIRED, 2014. Arvutivõrgus: https://www.wired.com/2014/04/your-big-data-is-worthless-if-you-dont-bring-it-into-the-real-world/ (08.03.2019)
48. M. Langemets jt (toim.). Eesti keele seletav sõnaraamat. „Tehisintellekt". Eesti Keele Sihtasutus 2009. Arvutivõrgus: http://www.eki.ee/dict/ekss/index.cgi?Q=tehisintellekt&F=M (02.02.2019)

49. M. Maarand. Ärisaladuse olemus ja tsiviilõiguslik kaitse lepinguvälistes võlasuhetes. Tartu Ülikool, Tallinn 2014, lk 18-19. Arvutivõrgus: http://dspace.ut.ee/handle/10062/42984 (07.04.2019)
50. M. McCole. This Smart Home Kit Relies on Sensors rather Than Cameras. WIRED. 2016. Arvutivõrgus: https://www.wired.com/2016/03/iotcookbook-smartthings/ (10.02.2019)
51. M. Oostveen. Identifiability and the applicability of data protection to big data. International Data Privacy Law, 2016, Vol. 6, No. 4. Arvutivõrgus: https://doi.org/10.1093/idpl/ipw012 (11.02.2019)
52. M. Perel, N. Elkin-Koren. Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement. Florida Law Review, vol 69. 2017. Arvutivõrgus: www.floridalawreview.com/wp-content/uploads/Perel_Elkin-Koren.pdf (14.03.2019)
53. M. Rosentau. Intellektuaalse omandi õigused infotehnoloogia valdkonnas. Infotehnoloogilise loomingu olemus. Juridica III/2008. Arvutivõrgus: http://juridica.ee/article.php?uri=2008_3_intellektuaalse_omandi_igused_infotehnoloogia_valdkonnas_infotehnoloogilise_loomingu_olemus (02.04.2019)
54. M. Rosentau. Intellektuaalse omandi õigused infotehnoloogias. Autori varalised õigused. Juridica X/2010. Arvutivõrgus: http://juridica.ee/article.php?uri=2010_10_intellektuaalse_omandi_igused_infotehnoloogias_autori_varalised_igused (04.04.2019)
55. M. Veale, L. Edwards. Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. Computer Law & Security Review. Volume 34, Issue 2, 2018, 398-404. Arvutivõrgus: https://doi.org/10.1016/j.clsr.2017.12.002 (25.03.2019)
56. P. Hustinx. Opinion of the European Data Protection Supervisor. Brüssel, 12.03.2014. Arvutivõrgus: https://edps.europa.eu/sites/edp/files/publication/14-03-12_trade_secrets_en.pdf (06.04.2019)
57. Riigikantselei. Eesti saab tehisintellekti strateegia. 27.03.2018. Arvutivõrgus: https://www.riigikantselei.ee/et/uudised/eesti-saab-tehisintellekti-strateegia (01.02.2019)
58. R. Kinkar. Tootjavastutus ja juhi deliktiõiguslik vastutus autonoomsete sõidukite tehnoloogia puudusest tingitud kahju tekkimise korral. Tartu: TÜ Õigusteaduskond 2015. Arvutivõrgus: http://dspace.ut.ee/bitstream/handle/10062/46852/kinkar_rauno.pdf (01.02.2019)
59. Seletuskiri ebaausa konkurentsi takistamise ja ärisaladuse kaitse seaduse eelnõu juurde 678 SE. 22.08.2018. Arvutivõrgus:

https://www.riigikogu.ee/tegevus/eelnoud/eelnou/9b6f21b8-db1c-436d-a045-326913d80d22 (05.04.2019)

60. Seletuskiri isikuandmete kaitse seaduse eelnõu juurde. 679 SE, 22.08.2018. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/5c9f8086-b465-4067-841e-41e7df3b95af (18.03.2019)
61. S. J. Russell, P. Norvig. Artificial Intelligence: A Modern Approach. Third Edition. New Jersey: Pearson Education Inc. 2010. Arvutivõrgus: http://aima.cs.berkeley.edu/ (02.02.2019)
62. S. K. Sandeen. The Cinderella of Intellectual Property Law: Trade Secrets. - P.K. Yu. Intellectual Property and Information Wealth: Issues and Practices in the Digital Age. Volume 2. Patents and Trade Secrets. Westport, Conn, London: Praeger, 2007
63. Sorainen. Sorainen võttis kasutusele Luminance'i tehisintellekti tehnoloogia. 25.10.2018. Arvutivõrgus: https://www.sorainen.com/et/sorainen-vottis-kasutusele-luminancei-tehisintellekti-tehnoloogia/ (01.02.2019)
64. S. Ranchordás. Book Review: The Black Box Society: The Secret Algorithms That Control Money and Information by Frank Pasquale, MA: Harvard University Press, 2015. Cambridge University Press, 2017. Arvutivõrgus: https://doi-org.ezproxy.utlib.ut.ee/10.1017/S1867299X00005894 (06.03.2019)
65. S. Shalev-Shwartz, S. Ben-David. Understanding Machine Learning: From Theory to Algorithms. Cambridge University Press, 2014. lk 268. Arvutivõrgus: https://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning (06.03.2019)
66. S. Zuboff. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology (2015) 30, 75–89. Arvutivõrgus: https://cryptome.org/2015/07/big-other.pdf (08.03.2019)
67. S. Wachter, B. Mittelstadt, L. Floridi. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. International Data Privacy Law, 2017, Vol. 7, No. 2. Arvutivõrgus: https://academic.oup.com/idpl/article-abstract/7/2/76/3860948 (25.03.2019)
68. T. Calders, B. Custers. What Is Data Mining and How Does It Work?, lk 28-29. 2. peatükk raamatust "Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases". Springer 2013, vol 3., lk-d 27 - 42. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)

69. T. Calders, I. Žliobaitė. Why Unbiased Computational Processes Can Lead to Discriminative Decision Procedures. 3. peatükk raamatust "Discrimination and Privacy in the Information Society: Data Mining and Profiling in Large Databases". Springer 2013, vol 3., lk-d 43-57. Arvutivõrgus: https://www.researchgate.net/publication/278661450_What_Is_Data_Mining_and_How_Does_It_Work (15.02.2019)
70. Tehisintellekt – e-keelenõu. Eesti Keele Instituut. 2013. Arvutivõrgus: http://kn.eki.ee/?Q=tehisintellekt (02.02.2019)
71. Tehisintellekt – IT Terministandardi sõnastik. Arvutivõrgus: http://www.keeleveeb.ee/dict/speciality/itstandard/dict.cgi?word=sv1482 (02.02.2019)
72. The European Commission's high-level expert group on artificial intelligence. A definition of AI: main capabilities and scientific disciplines. Definition developed for the purpose of the deliverables of the High-Level Expert Group on AI. Brüssel, 18.12.2018. Arvutivõrgus: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december.pdf (02.02.2019)
73. T. Klimas, J. Vaičiukaitė. The Law of Recitals in European Community Legislation. ILSA Journal of International & Comparative Law, Vol. 15, 2008. Arvutivõrgus: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1159604 (25.03.2019)
74. The Royal Society. Machine Learning: The Power and Promise Of Computers That Learn By Example. Arvutivõrgus: https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf (10.02.2019)
75. Written evidence submitted by Dr Alison Powell (ALG0067). 26.04.2017. Arvutivõrgus: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-andtechnology-committee/algorithms-in-decisionmaking/written/69121.html (18.03.2019)
76. Written evidence submitted by The Alan Turing Institute (ALG0073). 26.04.2017. Arvutivõrgus: http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/science-and-technology-committee/algorithms-in-decisionmaking/written/69165.html (18.03.2019)
77. Ärisaladus –M. Langemets jt (toim.). Eesti keele seletav sõnaraamat. Eesti Keele Sihtasutus 2009. Arvutivõrgus: http://www.eki.ee/dict/ekss/index.cgi?Q=%C3%A4risaladus&F=M (03.04.2019)

78. Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. 4., täiend. vlj. Tallinn: Juura, 2017
79. Y. Bathaee. The Artificial Intelligence Black Box And The Failure Of Intent And Causation. Harvard Journal of Law & Technology. Volume 31, Number 2, 2018. Arvutivõrgus: https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf (06.03.2019)

Õigusaktid

1. Autoriõiguse seadus – RT I, 19.03.2019, 54.
2. Ebaausa konkurentsi takistamise ja ärisaladuse kaitse seadus – RT I, 07.12.2018, 2.
3. Euroopa Liidu põhiõiguste harta – ELT C 326/391, lk 391-407.
4. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta – ELT L 281, lk 31 - 50
5. Euroopa Parlamendi ja nõukogu direktiiv 96/9/EÜ, 11. märts 1996, andmebaaside õiguskaitse kohta – ELT L 077, lk 20 - 28
6. Euroopa Parlamendi ja Nõukogu direktiiv 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK – ELT L 119/89, lk 1-18
7. Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/943, 8. juuni 2016, milles käsitletakse avalikustamata oskusteabe ja äriteabe (ärisaladuste) ebaseadusliku omandamise, kasutamise ja avalikustamise vastast kaitset – ELT L 157/1, lk 1-18
8. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta – ELT L 119/1, lk 1-88
9. Intellektuaalomandi õiguste kaubandusaspektide leping – RT II 1999, 22, 123.
10. Isikuandmete kaitse seadus – RT I, 04.01.2019, 11.
11. Ülemaailmse Intellektuaalse Omandi Organisatsiooni asutamise konventsioon – RT II 1993, 25, 55.

Kohtulahendid

1. RKTKo 11.10.2017, 2-16-1988
2. RKTKo 10.05.2017, 3-2-1-36-17
3. RKTKo 06.06.2012, 3-2-1-71-12
4. RKTKo 09.12.2008, 3-2-1-103-08
5. EK C-604/10, *Football Dataco jt*, kohtujurist P. Mengozzi ettepanek

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Jana Žuk,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

„Ärisaladuse ja isikuandmete kaitse regulatsiooni interaktsioon tehisintellekti läbipaistvuse tagamisel", mille juhendaja on professor Aleksei Kelli,

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, **30.04.2019**