MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO SAUGUMO AKADEMIJA

KORNELIJUS ZAKARAS
TEISĖ IR POLICIJOS VEIKLA
(SPECIALIZACIJA: IKITEISMINIS PROCESAS)

DIRBTINIO INTELEKTO NAUDOJIMO TEISĖSAUGOS INSTITUCIJŲ VEIKLOJE IŠŠŪKIAI ŽMOGAUS TEISIŲ POŽIŪRIU

Magistro baigiamasis darbas

Darbo vadovas: Prof. dr. Aurelija Pūraitė

Darbą atliko: Kornelijus Zakaras

Kaunas, 2021

TURINYS

SANTRUMPOS 3

ĮVADAS 4

1. DIRBTINIO INTELEKTO SĄVOKA, METODAI IR PRAKTINIS PRITAIKYMAS 8

1.1. Dirbtinio intelekto sąvoka 8

1.2. Dirbtinio intelekto istorinė raida 10

1.3. Pagrindiniai dirbtinio intelekto veiklos metodai 11

1.4. Dirbtinio intelekto raidos strategija Lietuvoje 13

1.5. Dirbtiniu intelektu pagrįstų sistemų naudojimas teisėsaugos institucijose 17

2. DIRBTINIO INTELEKTO TAIKYMAS TEISĖSAUGOS INSTITUCIJOSE 20

2.1. Dirbtino intelekto ir jo pagrindu sukurtos sistemos teisėsaugos institucijose. 20

2.2. Dirbtinio intelekto ir jo pagrindu sukurtos sistemos policijos institucijose 23

2.3. Dirbtino intelekto ir jo pagrindu sukurtų sistemų taikymas Valstybės sienos apsaugos tarnyboje 26

2.4. Dirbtinis intelektas ir žmogaus teisės teisėsaugos institucijų veikloje 28

2.4. Asmens teisių ir laisvių apsauga nuo dirbtinio intelekto keliamų pavojų 31

3. EMPIRINIS TYRIMAS „Dirbtinio intelekto naudojimo teisėsaugos institucijų veikloje iššūkiai žmogaus teisių požiūriu“ 35

IŠVADOS 49

PASIŪLYMAI: 51

LITERATŪRA: 52

PRIEDAI: 61

SANTRAUKA 70

SUMMARY 71

PATVRTINIMAS APIE ATLIKTO DARBO SVARANKIŠKUMĄ 72

SANTRUMPOS

DI – dirbtinis intelektas

EŽTK – Europos žmogaus teisių komisija

IT – Informacinės technologijos

VSAT – Valstybės sienos apsaugos tarnyba

UNICRI – United Nations Interregional Crime and Justice Research Institute (Jungtinių Tautų tarpregioninis nusikalstamumo ir teisingumo tyrimų institutas)

ĮVADAS

Nagrinėjamos temos aktualumas.

Dirbtinis intelektas (toliau - DI) – žmogaus sukurta technologinė sistema, prilygstanti bei imituojanti žmogaus intelektą, gebanti savarankiškai mokytis iš klaidų, analizuoti savo aplinką ir priimti savarankiškus sprendimus numatytiems tikslams pasiekti.[1] DI sistemos yra plačiai naudojamos interaktyviame pasaulyje, paieškos sistemose, skaitmeniniuose asistentuose, kompiuterinių žaidimų kūrime, apsaugos sistemose, taip pat teisėsaugos institucijose ir technikoje. Teisėsaugos institucijose DI sistemos pritaikomos procesų automatizavime (dokumentų analizėje, automatiškai suformuotose pranešimuose ir t.t.), transporto priemonėse (automatinių numerių nuskaityme, pažeidimų fiksavime), veido atpažinimo sistemose (oro uostuose, kertant valstybės sieną), robotuose (automatiniuose išminavimo robotuose, gatvių patruliuose) ir interneto technologijų aplinkoje. Šiuo metu yra skiriamos didelės investicijos ir resursai tiek Lietuvoje bei Pasaulio mastu siekiant tobulinti DI algoritmus ir panaudojimo galimybes[2] teisėsaugos institucijose ir įprastiniame žmonių gyvenime. DI ir technologijos leidžia daug tiksliau numatyti galimus nusikaltimus viešose vietose, taip pat gali padėti išaiškinti kitus nusikaltimus. Ankstesniu laikotarpiu tokių galimybių nebuvo, o panašioms prognozėms nustatyti reikėjo daug laiko ir žmogiškųjų išteklių. Sparčiai besivystant ir plačiai pritaikant DI technologija renkami ir naudojami dideli kiekiai asmens duomenų, o tai, neužtikrinant atitinkamų saugiklių ir priežiūros globaliu mastu, kelia iššūkius asmens teisei į privatumą ir duomenų apsaugą. Įvertinus tai, jog 90 % viso pasaulio duomenų buvo surinkti per pastaruosius penkerius metus.[3] Atitinkamas teisinių instrumentų adaptavimas reikalingas ir iš duomenų apsaugos reguliavimo perspektyvos. Teisė turi atspindėti žmonijos besikeičiančius tikslus. Nors investicijų į DI sistemas mastas ES vis dar neprilygsta galingiausioms šiuo požiūriu pasaulio valstybėms JAV ar Kinijai, tačiau ES vysto kryptingą politiką skaitmeninimo ir DI plėtros prasme.

Sugriežtintos duomenų apsaugos ir privatumo taisyklės ne tik pradėjo naują duomenų apsaugos reguliavimo etapą ES, bet kartu tapo pavyzdžiu bei atspirties tašku ir kitiems įstatymų leidėjams bei technologijų kūrėjams visame pasaulyje. Didėjant duomenų kiekiui, atsiranda didesni nesklandumai siekiant užtikrinti saugų ir tinkamą šių duomenų panaudojimą. Teisėsaugos institucijos tiek kaip DI vartotojos, tiek kaip visuomenės saugumą užtikrinantys

[1] Elijus Čivilis ir kt., „Lietuvos dirbtinio intelekto strategija. Ateities vizija“ *Ekonomikos ir inovacijų ministerija*, 2019 m. kovo 8 d., žiūrėta 2021 m. gruodžio 1 d., https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf

[2] *Ibid*

[3] The Royal Society. „Machine learning requires careful stewardship says“ 2017 m. balandžio 25 d., žiūrėta 2021 m. gruodžio 1 d., https://royalsociety.org/news/2017/04/machine-learning-requires-careful-stewardship-says-royal-society/

subjektai privalo imtis reikiamų priemonių, kad asmens teisės bei laisvės ir duomenų apsauga būtų maksimaliai užtikrintos.

Baigiamojo darbo aktualumas – pasirinkta baigiamojo darbo tema yra aktuali visoms tiek užsienio, tiek Lietuvos Respublikos teisėsaugos institucijoms, kurių veikoje yra taikomos DI technologijos bei sistemos. Visame pasaulyje plačiai diskutuojama apie DI, DI pagrindu veikiančias sistemas ir technologijas, dažniausiai pastebimi klausimai *„kokią DI teikia naudą?, kokios galimos DI grėsmės?, kaip DI pažeidžia numatytas teisės normas?“*. Šių klausimų analizavimas tampa vis platesnis, kadangi technologijų sritis kiekvieną dieną sparčiai plečiasi.

Ši tyrimo tema yra nauja, nes pastebima, kad DI sistemos bei technologijos pasauliniu mastu yra taikomos kiekviename asmens žingsnyje. Dėl šių veiksnių pasaulio valstybės aktyviai analizuoja ir sprendžia iškilusias problemas su tinkamu ir reglamentuotu DI taikymu kuo mažiau pažeidžiant teisėje numatytas normas.

Temos išskirtinumas — Lietuvoje DI veikiančių sistemų analizė ir tokių sistemų taikymas teisėsaugoje kol kas nėra plačiai analizuotas, tam tikrais aspektais (žmogaus teisėmis ir laisvėmis) ši tema yra plačiau analizuota užsienio literatūroje.

Baigiamojo darbo mokslinis naujumas — tema yra nauja ir aktuali dėl šiuo metu pasaulyje vykstančių technologinių pokyčių ir vertybinių transformacijų žmogaus teisių srityje. Šia tema pasauliniu lygmeniu yra analizuojama gan išsamiai, tačiau Lietuvoje tik pradedama plačiai išanalizuoti.

Darbo objektas — DI pagrindu veikiančių sistemų teisėsaugos institucijose taikymas žmogaus teisų požiūriu.

Darbo tikslas — atskleisti kilusius žmogaus teisių požiūriu iššūkius naudojant DI pagrindu veikiančias sistemas teisėsaugos institucijose.

Darbo uždaviniai:

1. Išnagrinėti DI sistemų bei technologijų istorinę raidą, DI sistemų tobulėjimą bei numatomą raidos strategiją;
2. Išanalizuoti, kokios galimos grėsmės kyla taikant DI pagrindu veikiančias sistemas bei technologijas teisėsaugos institucijose žmogaus teisių požiūriu;
3. Išnagrinėti DI pagrindu veikiančių sistemų bei technologijų praktinį taikymą teisėsaugos institucijose žmogaus teisių apsaugos kontekste.

Objektas — darbo objektą lemia analizuojamai temai atskleisti iškelti tikslai bei uždaviniai. Objektą sudaro teisėsaugos institucijų veikla taikant DI pagrindu veikiančias sistemas

ir technologijas. Apribota esminių ir didžiausius iššūkius procesams keliančių DI veiksmų analizė.

Metodologija

Duomenų analizė — šiame darbe šis tyrimo metodas taikytas analizuojant: 1) mokslinius straipsnius, susijusius su DI sistemomis ir technologijomis, DI sistemų pradmenis, vystymosi procesą. DI sistemų ir technologijų valdymu teisėsaugos institucijose; 2) DI reglamentuojančius teisės aktus, poįstatyminius teisės aktus, teisės aktų pasiūlymus.

Modeliavimas — šis metodas darbe taikytas modeliuoti nesudėtingus teisės aktų veikimo modelius realiose situacijose.

Lyginamasis — šis metodas darbe taikytas palyginti skirtingų DI sistemų ir technologijų praktinį pritaikymą.

Sisteminė analizė — šis metodas darbe naudotas aiškinantis DI sistemų veikimo principus, kaip DI sistemos ir technologijos veikia realiame gyvenime. Taikant vaizdo analizę, biometrinių duomenų analizę ir kitus veiksmus.

Interviu — šis metodas darbe taikytas apklausiant pasirinktus ekspertus: muitinės kriminalinės tarnybos pareigūnus, policijos departamento pareigūnus, pasienio rinktinės pareigūnus, civilius ekspertus. Jų atsakymai gali padėti tinkamai įvertinti DI sistemas bei šių technologijų naudojimą teisėsaugos institucijose ir fiziniame gyvenime apsaugant žmogaus teises.

Apibendrinimo — šis metodas darbe naudojamas skirtingų informacijos šaltinių apibendrinimui, taikomų DI sistemų teisėsaugos institucijose ir civiliniame gyvenime susijusiais žmogaus teisių aspektais.

Darbo struktūra — magistro baigiamąjį darbą sudaro 72 puslapiai. Darbą sudaro trys struktūrinės dalys. Pirmajame skyriuje pristatoma DI apibrėžtis, įvardijama sąvoka ir istorinė raida, analizuojami DI metodai ir jų taikymas, po to atkreipiamas dėmesys į strategiją ir pokyčius teisėsaugos institucijose. Antrajame skyriuje analizuojamas DI taikymas teisėsaugos institucijose, DI taikymas teisėsaugos institucijų veikloje. Taip pat antrajame skyriuje analizuojamas DI taikymas policijos veikloje, valstybės sienos apsaugos veikloje, analizuota DI ir žmogaus teisės teisėsaugos institucijų veikloje ir jų apsauga nuo DI keliamų pavojų. Trečiajame skyriuje atliekamas teisėsaugos institucijų ir technologų interviu apie dirbtinio intelekto naudojimo teisėsaugos institucijų veikoje, kokie iššūkiai kyla žmogaus teisių požiūriu ir konkrečių priemonių taikymu.

Ginamieji teiginiai:

1. DI pagrindu veikiančių sistemų bei technologijų intensyvi raida lemia žmogaus teisių ir laisvių užtikrinimo iššūkius.

2. DI pagrindu sukurtų sistemų taikymas teisėsaugos institucijose užtikrinant visuomenės saugumą dėl nepakankamo teisinio reguliavimo suponuoja kylančias grėsmes pažeisti pagrindines — žmogaus teises ir laisves.

1. DIRBTINIO INTELEKTO SĄVOKA, METODAI IR PRAKTINIS PRITAIKYMAS

1.1. Dirbtinio intelekto sąvoka

Prieš pradedant kalbėti apie dirbtinio intelekto (toliau - DI) naudą, pirmiausiai reikia aptarti dirbtinio intelekto sąvoką, pagrindinius kriterijus bei DI pagrindu sukurtų skaitmeninių sistemų vystymąsi. Mokslininkai neprieina vieningos nuomonės dėl DI sąvokos reikšmės, esama daug įvairių apibrėžimų, akcentuojančių skirtingus šio reiškinio elementus. Dirbtinio intelekto sąvoką pirmasis sugalvojo John McCarthy 1956 metais. Vystantis DI technologijoms, atsirado gilesnė dirbtinio intelekto sąvokos apibrėžimo problema. Pasak profesoriaus Marvin Minsky, DI yra mokslas pasitelkiantis mašininę funkciją atlikti užduotis, tačiau šios užduoties galutiniam atlikimui būtinas žmogaus intelektas.[4] Pagal kitą dirbtinio intelekto tyrinėtoją - Nils J. Nilson, DI yra veikla, skirta automatinių sistemų intelekto sukūrimui, o intelektas yra savybė, kuri leidžia sistemai tinkamai funkcionuoti atsižvelgiant į jos aplinką.[5] Pagal John McCarthy, DI yra akademinio ir komercinio darbo kompiuterinė sistema, apimanti mokslą ir inžineriją.[6] Tačiau vienas iš rimčiausiai tuometinių DI sąvoką tyrinėjusių mokslininkų buvo XIX amžiaus vidurio garsiausias Amerikiečių matematikas Alanas Tiuringas, savo straipsnyje „Computing Machinery and Intelligence“ apibrėžė skaitmeninio intelekto elgesį, sugebantį pasiekti žmogaus intelekto lygį bei pasiūlė apibrėžti DI: „kai kompiuteris sugebės įtikinti ir išspręsti mašininių sugebėjimų formuojantį testą prieš žmogų savo turimomis žiniomis bei galimybėmis, DI turės teisę būti vadinamas naujuoju kompiuteriu.“[7] Nuo to laiko vertinant kompiuterio intelektą ir sugebėjimus, naudojamas Tiuringo testas. Iki šių dienų dar joks mašininis įrenginys, turintis tinkamas galimybes, nėra įveikęs Tiuringo testo, tačiau yra manoma, kad ateis ta diena, kai DI įveiks Tiuringo testą ir tai bus nauja pradžia DI erai. Pagal minėtąjį testą, kompiuteris ar kitokia informacinė technologija būtų laikoma DI, jeigu žmogus, užduodantis tam tikrus klausimus kompiuteriui, gavęs atsakymus negalėtų atskirti, ar juos pateikė kompiuteris, ar žmogus. Tačiau DI nagrinėjęs žymus tyrinėtojas Niks John Nilsson teigė, jog DI remiasi multimediniu požiūriu, o tai reiškia, kad egzistuoja skirtumai tarp skaičiuotuvo ir žmogaus intelekto, tokie kaip:

- apimtis,

[4] Marvin Minsky, „The Emotion Machine“ *Simon & Schuster*, 1/1 (2007): 3-7, žiūrėta 2021 m. gruodžio 1 d., https://www.simonandschuster.com/books/The-Emotion-Machine/Marvin-Minsky/9780743276641
[5] Peter Stone ir kt., „Artificial Intelligence and life in 2030“ *Stanford University*, 1/1 (2016): 4-16, žiūrėta 2021 m. gruodžio 1 d., https://apo.org.au/sites/default/files/resource-files/2016-09/apo-nid210721.pdf
[6] Michael Mills, „Artificial intelligence in law: the state of play 2016“, 1/1 (2016): 1-6, žiūrėta 2021 m. gruodžio 1 d., https://www.neotalogic.com/wp-content/uploads/2016/04/Artificial-Intelligence-in-Law-The-State-of-Play-2016.pdf
[7] Stone ir kt. *op. cit., 5-15*

- greitis,
- autonomiškumo lygis,
- gebėjimas apibendrinti.[8]

Šis DI apibūdinimas implikuoja, kad pilnaverčiam DI veikimui neužtenka vien programinio algoritmo. Jam reikia ir kitų savybių, kurias turi tik gyvo žmogaus organizmas, tokių kaip jausmai, intuicija.

Kiti šaltiniai teigia, kad dirbtinis intelektas – tai bet koks dirbtinai sukurtas intelektas, t. y. programinė sistema su įvairiais įvestiniais algoritmais, taip imituojant žmogaus mąstymą kompiuteryje. Tačiau DI skiriasi nuo įprastų kompiuterinių algoritmų tuo, kad gali pats save apmokyti, ir dėl to, atlikdamas tą patį veiksmą, gali elgtis kitaip, priklausomai nuo prieš tai atliktų veiksmų. Tai labai panašu į veiksmus, kai žmogaus turi sukaupęs tam tikrą patirtį ir priima atitinkamus sprendimus. Tokie metodai suteikia daugiau lankstumo ir leidžia sukurti programas, galinčias suprasti ir turėti tam tikrą patirtį, tai yra, turinčias žmogaus intelekto bruožų.

Atkreiptinas dėmesys į teorinę prognozę, kad 2047 metais dirbtinio intelekto sistemos pasieks žmogaus mąstymo lygį, o galbūt net ir pralenks.[9] Tai kol kas tik prielaida, kad kompiuteriai gali pakeisti žmogų ar net tapti atskiru teisės subjektu, tačiau jau dabar galime pastebėti, jog vis daugiau kasdieninių žmogaus darbų atlieka automatinės sistemos. Nors pasaulis vis dar ankstyvojoje intelektinių technologijų plėtros stadijoje, tačiau ateityje yra prognozuojami du scenarijai: pirmasis – kompiuteris ir toliau vykdys tik riboto skaičiuotuvo funkcijas, antrasis – kompiuteriai taps protingesni už žmogų ir bus naudojami įvairiose gyvenimo srityse.[10]

Apibendrinant galima teigti, kad DI remiasi žiniomis apie žmogaus mąstymo procesus, juos imituoja, tačiau vis dar neturi tam tikrų žmogui būdingų intelektinių savybių. Panašu, kad šiuo metu, DI kūrėjai nusiteikę entuziastingai ir siekia patvirtinti prielaidą, kad žmogaus smegenų darbas iš esmės nesiskiria nuo kompiuterio, todėl sukūrus pakankamą kiekį neuronų analogų, galima sukurti žmogui tapačią intelekto kopiją, su pasižyminčiomis tokiomis intelektinėmis veiklomis, kaip patirtimi paremti savarankiški sprendimai, individualūs norai bei fantazijos.

[8] Peter Stone ir kt., „Artificial Intelligence and life in 2030“ *Stanford University*, 1/1 (2016): 4-16, žiūrėta 2021 m. gruodžio 1 d., https://apo.org.au/sites/default/files/resource-files/2016-09/apo-nid210721.pdf
[9] Dom Galeon, „Softbank CEO: The Singularity Will Happen by“ 1/1 (2017): 1, žiūrėta 2021 m. gruodžio 1 d., https://futurism.com/softbank-ceo-the-singularity-will-happen-by-2047
[10] Richard Susskind, „The End Of Lawyers? Rethinking The Nature Of Legal Services“ 1/1 (2010): 25-49, žiūrėta 2021 m. gruodžio 1 d., https://www.goodreads.com/book/show/3075321-the-end-of-lawyers

1.2. Dirbtinio intelekto istorinė raida

Žavėjimasis mąstančiomis mašinomis prasidėjo labai seniai. Kaip teigia T. Wischmeyer ir T. Rademacher, dar senovės Egipte buvo žinoma Amono statula, kuri galėjo pakelti ranką ir kalbėti[11]. Pirmos skaičiavimo mašinos buvo pradėtos gaminti dar Antikoje ir bėgant laikui vis tobulinamos. XX amžiaus viduryje skaičiavimo mašinos ir pirmieji kompiuteriai buvo labai masyvūs, be galo brangūs ir turėjo mažiau galios negu šiuolaikiniai laikrodžiai. Tada jie manipuliavo tik skaičiais, bet keletas mokslininkų padarė išvadą, kad jie galėtų manipuliuoti ir simboliais, o tai jau būtų panašiau į žmogiškąjį mąstymą. 1956 m. buvo surengta pirmoji mokslinė konferencija apie DI , kur šitas terminas ir buvo sugalvotas Džono McCarthy. 1956 — 1974 metai laikomi auksiniu DI amžiumi, atradimų amžiumi.[12] Programos, kurios buvo sukurtos, tuo metu daugumai žmonių atrodė tiesiog nuostabios. Kompiuteriai sprendė algebros problemas, įrodinėjo geometrijos teoremas ir mokėsi kalbėti. Keletas didžiausių tuometinių XIX amžiaus atradimų, kurių pagalba buvo išspręstos 38 iš 52 matematinių teoremų, 1956 — 1974 metais buvo sukurtas pirmasis pokalbių robotas, o vėliau Japonijoje pristatytas pirmasis panašius bruožus į žmogų turintis robotas.[13] Tuo metu tik nedaugelis tikėjo, kad toks protingas mašinų elgesys iš viso gali būti įmanomas. Tuometiniai tyrinėtojai optimistiškai prognozavo, kad po mažiau nei 20 metų bus sukurta DI mašina. Tačiau to nepavyko padaryti, nes aštuntajame dešimtmetyje DI tapo kritikos objektu. Daugiau nei po pusės amžiaus DI sėkmingai pradėtas naudoti technologijų pramonėje. 1997 metais „Deep Blue“ tapo pirmąja šachmatais sugebančia žaisti sistema, kuri nugalėjo tuometinį pasaulio šachmatų čempioną Garry Kasparovą.[14] Pradėti taikyti pirmieji išmanūs įrenginiai, veikiantys tiesiogiai žmogui jų nekontroliuojant. Taip pat XIX amžiaus pabaigoje Ernst Dickman sukurta mašina be jokio žmogaus nuvažiavo 158 kilometrus, pasiekdama 180 km/val. greitį. Keičiantis tūkstantmečiui buvo sukurti pirmieji sudėtingi vaikštantys robotai.[15] Visa dirbtinio intelekto raida pavaizduota 1 pav., kuris parodo DI tobulėjimą.

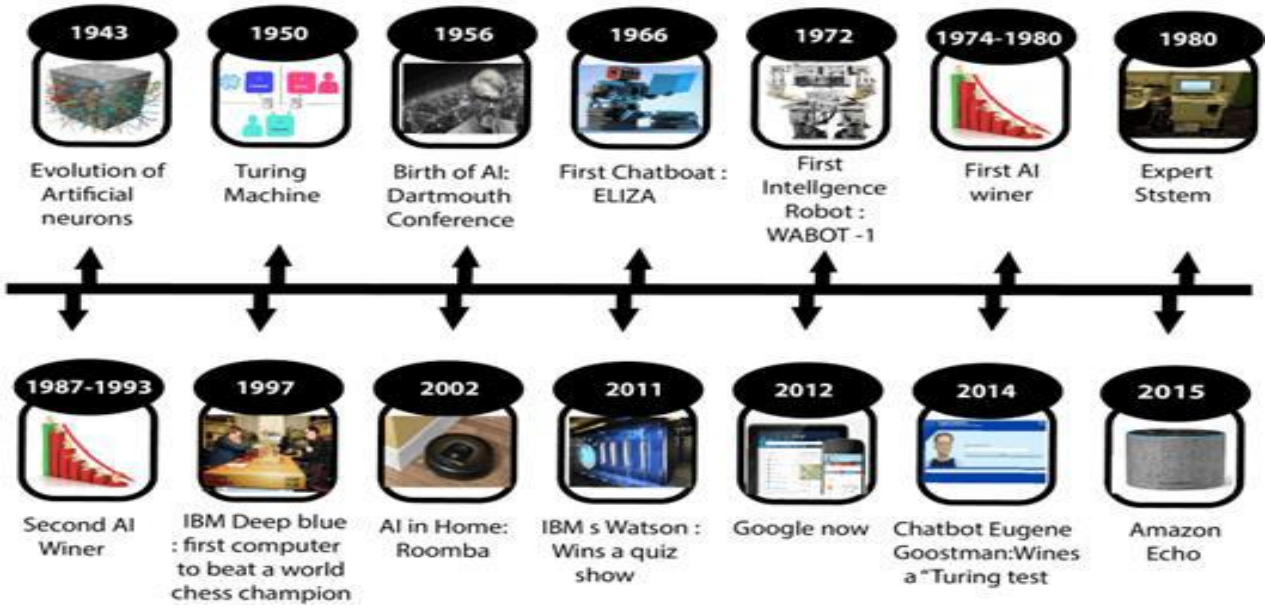
[11] Thomas Wischmeyer ir Timo Rademacher, „Artificial intelligence and healthcare“ *Springer* 1/1, (2020): 307-321, žiūrėta 2021 m. gruodžio 1 d., https://books.google.lt/books?id=FQ3BDwAAQBAJ&lpg=PA307&ots=f2eVC4HnCr&dq=Artificial%20intelligence%20and%20healthcare%3A%20procedures.%20In%3A%20T.%20Wischmeyer%20and%20%20T.%20Rademacher&hl=lt&pg=PA307#v=onepage&q&f=false

[12] *Ibid*

[13] „Journal of Law & Technology“, *AI Time Popular Articles*, 2020 m. sausio 9 d., žiūrėta 2021 m. gruodžio 1 d., https://www.ijsr.net/gettop10count.php

[14] Thomas Wischmeyer and Timo Rademacher, „Artificial intelligence and healthcare“ op. cit.

[15] *Ibid*



1 pav. Dirbtinio intelekto istorinė laiko juosta: 1943 m. dirbtinių neuronų evoliucija; 1950 m. Tiuringo mašina; 1956 m. dirbtinio intelekto gimimas: „Dartmounth" konferencija;1966 m. pirmasis pokalbių botas „ELIZA"; 1972 m. pirmasis intelektinis robotas „WABOT-1"; 1974 - 1980 m. pirmasis dirbtinio intelekto nuosmukis; 1980 m. ekspertinė sistema; 1983-1993 antrasis dirbtinio intelekto nuosmukis; 1997 m. IBM kompiuteris įveikia pasaulio šachmatų čempioną; 2002 m. dirbtinis intelektas namuose; 2011 m. kompiuteris laimėjo protų mūšį ; 2012 m. dabartinis „Google". 2014 m. robotas įveikia Turingo testą; 2015 m. Amazon parduotuvės sukurtas virtualus asistentas.[16]

Apibendrinat galima sakyti, kad DI nėra sukurtas žmogaus intelekto pakaitalas. Tai žmonių sukurta programinė įranga.[17] Kuri atlieka įvestas tam tikras funkcijas. Nesibaigiantį DI potencialą ir jį lydinčius vis naujus sprendimus verta analizuoti itin atidžiai, įsigilinus į kiekvieną konkretų DI sistemų taikomą metodą. DI gali būti tobulinamas atskirais segmentais, o ne kaip vientisa sistema.

1.3. Pagrindiniai dirbtinio intelekto veiklos metodai

Nuo senų laikų mokslininkai ieškojo būdų, kaip padaryti mašininius įrenginius kuo labiau išmanesniais. Įvairiais laikotarpiais vis atsirasdavo žmonių, pateikiančių naujų idėjų. Tačiau šios suskildavo į atskiras šakas, nes kažkas nukopijuodavo svetimas idėjas.[18] Kiekviena iš DI plėtros krypčių savaip svarbi ir pritaikoma įvairiose žmogaus veiklos srityse. Verta aptarti pagrindinius metodus, dažniausiai naudojamus DI valdomuose procesuose:

Planavimas (*angl. Planning*) – tai metodas, kai į kompiuterį įvedamas laukiamas rezultatas ir dabartinė padėtis. Kompiuteris, automatiškai peržiūrinėdamas visus galimus variantus ir atmesdamas neteisingus, bando surasti optimalų kelią tikslui pasiekti. Pagal turimus

[16] Alex Castrounis, „Brief history of artificial intelligence." 2020 m. vasario 23 d., žiūrėta 2021 m. gruodžio 1 d., https://www.psdtolive.com/the-history-of-artificial-intelligence/

[17] Europos Komisija „Europos Komisijos Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais sukurtoje DI apibrėžtyje" 2018 m. gruodžio 7 d., 795 galutinis, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0011.02/DOC_2&format=PDF

[18] „Journal of Computer Engineering (IOSR-JCE)" *IOSR*, 2015 m. gegužės 31 d., žiūrėta 2021 m. gruodžio 1 d., https://www.iosrjournals.org/#school-overview

duomenis dažniausiai sudaromas sprendimo algoritmas – teisingų veiksmų seka. Tokios sistemos pavyzdys gali būti veikianti šachmatų mašina, kuri turėdama visas šachmatų ėjimo kryptis gali be vargo laimėti net ir prieš profesionalų žaidėją.[19]

Mašininis mokymasis (*angl. Machnie learning*) – tai metodas, kuris sukuria sistemą, galinčią pačiai save tobulinti savarankiškai papildant duomenų bazę identifikuotomis klaidomis. Jau dabar yra keletas tokių programų, tačiau jų galimybės kol kas yra labai ribotos. Ideali sistema privalo mokėti atpažinti ir analizuoti tekstą, susijungti su internetu ir naršyti jo platybėse ieškant informacijos nuolatiniam tobulinimuisi.[20]

Automatinis programavimas (*angl. Automatic programming)* – tai metodas, kurio pagalba kompiuteris, kuriam duotas uždavinys, pats sukuria sau programą to uždavinio išsprendimui ir susikuria algoritmą kitiems panašaus pobūdžio uždaviniams atpažinti bei išspręsti.[21]

Šablono atpažinimas (*angl. Template recognition*) – tai metodas, dažniausiai naudojamas vaizdų atpažinimui bei įvairiose teisėsaugos institucijų taikomose skaitmeninėse sistemose. Nufilmuotą ar nufotografuotą vaizdą programa nuolat lygina su duomenų bazėse esančiais šablonais ir nustačiusi sutapimus arba klaidingai nurodytus duomenis atitinkamai reaguoja.[22]

Išvada (*angl. Conclusion*) – tai priešingybės metodas, kai programa priima tam tikrą sprendimą ir laiko jį vieninteliu teisingu, kol nėra įrodyta priešingai arba nėra sukuriama kita panaši išvada.[23]

Žinių reprezentacija (*angl. Knowledge representation*) – tai metodas, kurio pagrindu yra sukuriama programa bei tam tikras programinis algoritmas, kuris, turėdamas išsaugotas įvairias žinias bei žodžius, išverčia į duomenis suprantama kompiuteriui kalba.[24]

Neuroniniai tinklai (*angl. Neural networks*) – tai metodas, kuris veikia tais pačiais principais kaip ir žmogaus smegenyse esantys neuronų tinklai. Tai dažniausiai yra didžiulis kiekis tarpusavyje susietų paprastų procesorių, sąveikaujančių vienas su kitu ir sugebančių keisti savybes priklausomai nuo pageidaujamo rezultato. Tokiu metodu galima spręsti praktiškai bet

[19] Miquel Garrich Alabarce ir Pablo Pavon Marino „Artificial intelligence (AI) methods in optical networks“ *Optical Switching and Networking*, 1/1, (2018): 43-57, žiūrėta 2021 m. gruodžio 1 d., https://doi.org/10.1016/j.osn.2017.12.006
[20] *Ibid*
[21] *Ibid*
[22] *Ibid*
[23] *Ibid*
[24] *Ibid*

kokias skaičiavimo ir logines operacijas. Tačiau pilnaverčio smegenų modelio sukūrimui prireiktų žymiai daugiau kompiuterių nei dabar iš viso yra pasaulyje.[25]

Euristika (*angl. Heuristics*) – tai metodas, kai yra identifikuojamos visos galimos situacijos. Jos testuojamos ir pašalinant neefektyvius užduočių sprendimo būdus ir taip nustatomas optimalus bei priimtinas sprendimas. Tai labai panašu į „Planavimo“ metodą, tačiau čia kompiuteris pats modeliuoja galimus įvykių sprendimo variantus.[26]

Genetiniai algoritmai (*angl. Genetic algorithms*) – tai metodas, veikiantis kaip evoliucijos procesas gamtoje. Programavimo kalba parašomos kelios programos, kurios tarpusavyje sukryžminamos – ir taip susidaro daugybė alternatyvių programų, kurios, savo ruožtu, pakartoja tą patį veiksmą. Iš gautų milijonų kombinacijų atrenkamos tos, kurios labiausiai atitinka uždavinio sąlygas.[27]

Be šių minėtų metodų dabartinis DI veikimo modelis taptų nesuprantamas ir keliantis dideles diskusijas, nors šios DI apibrėžties paradigmos nėra baigtinės. Aptartos pagrindinės DI plėtros gairės padeda suvokti, kas ir kaip vyksta su DI, kokios būsimos pagrindinės DI kryptys. Keletas pačių svarbiausių metodų, be kurių teisėsaugos institucijoms būtų žymiai sudėtingiau dirbti yra šie:

- Planavimas
- Automatinis programavimas
- Šablono atpažinimas
- Neuroniniai tinklai
- Genetiniai algoritmai

Šie metodai, atlikdami sau priskirtas funkcijas, teikia pagalbą ir supaprastina teisėsaugos institucijų darbą bei tausoja finansinius resursus. Pasitelkiant reikiamus metodus, galima užkirsti kelią būsimiems įvairaus pobūdžio nusikaltimams, palengvinti esamų nusikaltimų ištyrimą.

1.4. Dirbtinio intelekto raidos strategija Lietuvoje

DI yra vienas iš strateginių XXI amžiaus technologijų, kurios teikiama nauda pasaulio ekonomikoms yra neabejotina. Be kita ko, DI taikomosios programos pagerino sveikatos priežiūrą, padidino ūkininkavimo veiksmingumą, prisidėjo prie klimato kaitos švelninimo ir

[25] Miquel Garrich Alabarce ir Pablo Pavon Marino „Artificial intelligence (AI) methods in optical networks“ *Optical Switching and Networking*, 1/1, (2018): 43-57, žiūrėta 2021 m. gruodžio 1 d., https://doi.org/10.1016/j.osn.2017.12.006
[26] *Ibid*
[27] „Journal of Computer Engineering (IOSR-JCE)“ *IOSR*, 2015 m. gegužės 31 d., žiūrėta 2021 m. gruodžio 1 d., https://www.iosrjournals.org/#school-overview

prisitaikymo, taip pat pagerino gamybos efektyvumą, išplėtojo teisėsaugos institucijų galimybes visuomenės saugumo užtikrinimui. Todėl kalbant apie DI kaip technologijų, „kurias taikant derinami duomenys, algoritmai ir kompiuterijos pajėgumai“[28] visumą, galima sakyti, kad tai itin naudinga visuomenei sukurta sistema, kuri palengvina darbus įvairiose srityse. Šios technologijos pagerina darbo efektyvumą, apdoroja didelius kiekius pateikiamos informacijos, pažymi ir atrenka netikslumus, o tai skatina didesnį tobulėjimą. Tai pažymima ir Europos Komisijos „Baltojoje knygoje“ apie DI kompetencijas, kurios pasižymi kaip „kompiuterijos pažanga ir didėjantis duomenų prieinamumas yra pagrindiniai veiksniai, lemiantys dabartinį DI pakilimą.“[29] Europos Komisijos „Baltojoje Knygoje“ apie DI pažymima, kad DI grindžiamas didelio kiekio duomenų apdorojimu, įskaitant asmens duomenis, jų rinkimu, analize ir pasikartojančiu kaupimu iš įvairių šaltinių.[30] Tačiau būtina nepamiršti, kad norint pasiekti reikiamus ir tikslius rezultatus duomenų informacijos apdorojime, svarbu, jog, „taikant automatizuotą šių duomenų tvarkymą, pasitelkiami kompiuteriniai algoritmai ir pažangios duomenų apdorojimo technologijos.[31] Pagal šiuos algoritmų metodus naudojami, saugomi ir perduodami duomenys siekiant sukurti tam tikrus kartotinius veiksmus, kurių pagalba atsirastų galimybė nustatyti naujausias tendencijas ir reikiamus modelius. DI duomenys gaunami ne tik tiesiogiai iš asmenų pateikiamos informacijos. Jie gaunami iš jų veiksmų, tam tikrų poelgių, kurie palieka žymę skaitmeninėje erdvėje. Pagrindinė naudojama informacija gaunama taikant DI programas, daugiausia informacijos surenkama iš pramonės, taip pat verslo ir viešojo sektoriaus naudojamų duomenų, renkamų, tvarkomų įvairiausiais tikslais.

Kalbant apie DI padėtį Lietuvoje ekonomikos požiūriu, ji yra gana išskirtinė. Anot McKinsey, Lietuva patenka į šalių su „vidutiniais ekonomikos pamatais“[32] grupę. Tai reiškia, kad net esant silpnesnei ekonominei situacijai nei aukštesnės kategorijos šalyse (pavyzdžiui Švedijoje, Belgijoje), DI vis tiek turi galimybę daryti didelį ekonominį poveikį Lietuvoje. DI augimas Lietuvoje turėtų būti sutelktas į reikšmingiausius sektorius, tokius kaip pramonė, teisėsauga ir t.t. Šie sektoriai nustatyti vadovaujantis dviem veiksniais – reikšmės Lietuvos ekonomikai ir verslui bei visuomenės saugumui. Tačiau dabartiniu laikotarpiu didelio valstybės strateginio požiūrio ir reikšmingų investicijų į DI plėtros sistemas nėra, tačiau yra įtvirtintos

[28] Europos Komisija „Baltoji Knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ 2020 m. vasario 19 d., 65 galutinis. žiūrėta 2021 m. gruodžio 1 d., https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf
[29] *Ibid*
[30] *Ibid*
[31] *Ibid*
[32] Mckinsey&Company, „Want to improve consumer experience?“ *Collaborate to builda a product data standard.* 2020 m. Balandžio 15 d., žiūrėta 2021 m. gruodžio 1 d., https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/want-to-improve-consumer-experience-collaborate-to-build-a-product-data-standard

kelios priemonių, kuriomis pasinaudojus DI technologijų raida Lietuvoje sparčiai patobulėtų.[33] Tai, pavyzdžiui, būtų skiriamos papildomos investicijos DI plėtrai, tokiu atveju valstybė pasiektų didesnius plėtros rodiklius. Šiuos rodiklius būtina paminėti bei aptarti plačiau, į kuriuos privalėtų būti atsižvelgiama, apibūdinama esama situacija ir nurodoma, kokia linkme reiktų judėti, norint pasiekti tam tikrus rezultatus:

1. Padidinti skaitmeninių sistemų naudojimą privačiame sektoriuje. Tai reiškia, kad reikia išanalizuoti galimybę vystyti DI viename iš Lietuvoje naujai įsteigto skaitmeninių naujovių centrų. Taip pat skatinti naujai steigiamas įmones, ypač inovatyvius startuolius, diegti DI programas. Kaip paskatą naujų sistemų steigimui, įmonėms galėtų būti įteikiamas DI ženklelis, įrodantis jų lyderystę skaitmeninėje srityje. Šiam įvertinimui pasiekti galėtų būti teikiama valstybės parama, įvairūs sisteminiai mokesčių palengvinimai. Taip pat būtina skatinti DI vystytojus sukuriant naują Lietuvos DI vystymo centrą.[34] Šiomis skatinimo priemonėmis galima padėti Lietuvos privataus sektoriaus subjektams, veikiantiems DI plėtros srityje, pasiekti ES lygmenį. Puikus pavyzdys, Lietuvoje įkurta įmonė „Vinted“ pritraukė dideles investicijas[35]. Taip pat visiems gerai žinoma įmonė „TransferGo“, veikianti DI pagrindu, pritraukė taip pat dideles investicijas Lietuvai. Nuolatiniam DI sistemų augimui privačiame sektoriuje reikalingi moksliniai tyrimai bei plėtra infrastruktūroje. Kadangi privatus sektorius dažniausiai yra žingsniu priekyje lyginant su viešuoju sektoriumi, atsižvelgiant į pasaulinę padėtį krašto apsaugos sistemoje, naudojamos sistemos ir įrankiai, taip pat ženkliai pažangesni už kitų sričių naudojamas sistemas. Reikalinga skatinanti privatų sektorių kurti DI sistemas, kurios padėtų modernizuoti ir viešojo sektoriaus institucijų veiklą. Mano nuomone, privatus sektorius privalo bendradarbiauti su viešojo sektoriaus institucijomis, nes pastarosios turi labai ribotus finansinius ir žmogiškuosius išteklius DI sistemų kūrimui ir tobulinimui. Taip pat Lietuvos strategijoje reiktų numatyti ir atskirai įvertinti DI plėtrą būtent viešajame sektoriuje.

2. Viešajame sektoriuje, kalbat apie DI sistemų naudojimą, numatoma sukurti atitinkamą inovacijų kultūrą viešajame sektoriuje, skatinančią kurti, diegti ir išbandyti DI sprendimus. Tam būtina sukurti valstybės reguliuojamą testavimo prieigą, įgalinančią naudoti ir išbandyti DI sistemas viešajame sektoriuje ribotą laiko tarpą. Taip DI sistemų kūrėjai galėtų išmėginti savo produktą realioje aplinkoje, o viešasis sektorius galėtų nuspręsti, kokie

[33] Europos Sąjungos Taryba, „Komisija komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ 2021 m. balandžio 29 d., 205 galutinis. žiūrėta 2021 m. gruodžio 1 d., https://data.consilium.europa.eu/doc/document/ST-8334-2021-INIT/lt/pdf

[34] Čivilis ir kt., „Lietuvos dirbtinio intelekto strategija. Ateities vizija“ *supra note,* 6-7

[35] Jovita Budreikienė ir Paulius Grinkevičius, „Lietuvos startuoliai šiemet pritraukė 420 mln. Eur investicijų“ *Verslo žinios,* 2021 m. spalio 29 d., žiūrėta 2021 m. gruodžio 1 d., https://www.vz.lt/inovacijos/2021/10/29/lietuvos-startuoliai-siemet-pritrauke-420-mln-eur-investiciju

sprendiniai turėtų būti integruoti darbo rezultatams ir produktyvumui gerinti[36]. Būtina skatinti viešąsias įstaigas diegti DI sistemas, skirtas ne tik viešųjų paslaugų visuomenei teikimui, bet ir galinčias įvertinti bei optimizuoti darbo srautą. Vienas iš siūlymų, pateiktų Lietuvos DI vystytojų, tokių kaip „AI Boost Lithuania“, yra įsteigti Lietuvos DI patariamąją valdybą, padėsiančią vyriausybei priimti sprendimus dėl DI politikos tiek viešajame, tiek privačiame sektoriuje.[37] Šios valdybos vienas iš tikslų būtų rengti diskusijas, susijusias su platesniu DI sistemų panaudojimu viešajame ir privačiajame sektoriuje, taip pat ieškoti įvairių investicinių šaltinių, kad skaitmeninės programos galėtų tinkamai veikti ir būtų prieinamos visoms institucijoms. Ši valdyba galėtų veikti tiek valstybiniu, tiek tarptautiniu lygmenimis platesniam bei produktyvesniam DI pritaikymui praktikoje atsižvelgiant į pagrindines ekonomikos raidos tendencijas.[38]

3. Kita strateginė kryptis siekiant spartesnės DI plėtros yra pagrindinių ekonomikos sektorių, potencialiai gausiančių daugiausiai naudos iš DI sistemų pritaikymo Lietuvos bei Europos mastu, identifikavimas ir kryptingas sistemų kūrimas atsižvelgiant į šių sektorių poreikius. Norint gauti didesnės naudos rekomenduojama sukurti individualius DI naujovių pritaikymo metodus gamybos, žemės ūkio, sveikatos priežiūros, transportavimo ir energetikos, teisėsaugos sektoriams.[39] Viena iš paminėtinų specifinių DI pritaikymo sričių yra teisėsaugos institucijos, kuriose DI integracija yra itin reikšminga, nes padėtų užtikrintų saugesnę aplinką Lietuvoje.[40] Galima paminėti vieną iš strateginių projektų, įgyvendinamų Lietuvoje — „Asmens teisių įgyvendinimo iššūkiai modernioje visuomenėje: naujų ir besikeičiančių teisių dilemos“ programa, kurį parengė Lietuvos Respublikos švietimo, mokslo ir sporto ministerija. Šioje programoje numatomi konkretūs uždaviniai, kuriuos turės pasiekti Lietuvos socialinių mokslų centras. Programoje yra numatomi veiklos tikslai: „tirti teisinius iššūkius, su kuriais susiduria moderni visuomenė, kintant jau įsitvirtinusių asmens teisių turiniui bei atsirandant naujos kartos asmens teisėms, ir pateikti pasiūlymus tolesnei teisinės sistemos raidai.“[41] Šis tikslas indikuoja, jog Lietuva yra pasiryžusi įvairiomis priemonėmis skatinti bei šviesti žmones apie jų galimas žmogaus teises programinėje įrangoje. Ši programa gali suteikti tyrimams kryptingumo ir

[36] Čivilis ir kt., „Lietuvos dirbtinio intelekto strategija. Ateities vizija“ *supra note,* 8-7
[37] „Europos komisija siūlo naujas su kompetencija ir pasitikėjimu dirbtiniu intelektu susijusias taisykles ir veiksmus“ *Teise.Pro* 2021 m. kovo 21 d., žiūrėta 2021 m. gruodžio 1 d., https://www.teise.pro/index.php/2021/04/21/ek-siulo-naujas-su-kompetencija-ir-pasitikejimu-dirbtiniu-intelektu-susijusias-taisykles-ir-veiksmus/
[38] Čivilis ir kt., op. cit., 6-7
[39] *Ibid*
[40] *Ibid*
[41] Lietuvos Respublikos švietimo, mokslo ir sporto ministro įsakymas Nr. V-871 „Asmens teisių įgyvendinimo iššūkiai moderniojo visuomenėje: naujų ir besikeičiančių teisių dilemos“ 2021 m. gegužės 25 d., žiūrėta gruodžio 1 d., https://www.smm.lt/uploads/documents/mokslas/tarptautinis_bendradarbiavimas/LSMC%20TI%20Ilgalaike%20programa%20Asmens%20teises.pdf

nuoseklumo,[42] nes bus sukuriama erdvė sistemiškiems tyrimams žmogaus teisių srityje įvertinant skaitmeninių technologijų įtaką šių teisių paradigmos kaitai.

Minėtoms strategijoms įgyvendinti Lietuvoje yra suformuotas ilgalaikis investicijų planas. Šis planas numato subalansuotą ekonomikos plėtrą panaudojant ne tik nacionalinius, bet ir ES finansavimo šaltinius. Atskiroms DI strategijos kryptims yra parengti atskiri priemonių planai, kuriuose numatyti užsibrėžti rezultatai. Šiems rezultatams pasiekti yra numatyti įgyvendinimo laikotarpiai bei skirtos lėšos ir atsakomybė dėl šių rezultatų neįvykdymo[43].

1.5. Dirbtiniu intelektu pagrįstų sistemų naudojimas teisėsaugos institucijose

DI kuriamos programos ir algoritmai keičia pasaulį prieš mūsų akis. DI pagrįstos sistemos jau geriau negu medicinos specialistai diagnozuoja tam tikras ligas. Taip pat DI sparčiai integruojamas ir teisėsaugos institucijose vykdant jų atliekamas funkcijas. Tačiau reikia nepamiršti, kad DI taip pat gali turėti ir neigiamą poveikį. Pavyzdžiui, dėl DI sistemų netinkamai surinktų duomenų, gali atsirasti didelė žala žmogaus teisėms, nes tai priklauso nuo didelio duomenų kiekio rinkimo ir jų galimų klaidų analizės metu. Atlikus tinkamą duomenų analizę, daugeliu atveju būtų galima išsaugoti esamus apsisaugoti nuo šališkumo ir diskriminacijos modelių.

Būtina paminėti, kad „kuriant bei plėtojant taip pat diegiant ir naudojant DI turi būti visapusiškai laikomasi pagrindinių teisių ir esamų teisinių taisyklių.[44] Tiek skaitmeniniame, tiek fiziniame pasaulyje turėtų būti užtikrinama tokio paties lygio DI naudojimo apsauga. Tokiu apsaugos standartu pagal Europos Sąjungos pagrindinių teisų chartijos 52 straipsnio 1 dalį, laikytinas bet koks šios Chartijos pripažintų teisių ir laisvių įgyvendinimo apribojimas, remiantis proporcingumo principu, galimas tik tuo atveju, kai jis būtinas ir tikrai atitinka Europos Sąjungos pripažintus bendrus interesus arba reikalingus kitų teisėms ir laisvėms apsaugoti, taip pat turi būti numatytas įstatymo ir nekeisti šių pagrindinių teisių ir laisvių esmės.[45]

Dėl šių galimybių atsirado didelis judėjimas, siekiantis įterpti asmens intelektą į DI sritį. DI parodo didelę žmogaus teisių ir įstatymų naudą vertinant bei sprendžiant sudėtingą poveikį visuomenei.[46] Reikia pažymėti ir tai, kad skaitmeninės technologijos, prie jų priskiriant

---

[42] Lietuvos Respublikos švietimo, mokslo ir sporto ministro įsakymas Nr. V-871 „Asmens teisių įgyvendinimo iššūkiai moderniojo visuomenėje: naujų ir besikeičiančių teisių dilemos“, *supra note*, 3

[43] „Lietuva po COVID-19: investicijos, kurios keis ekonomikos DNR“ *Mano vyriausybė*, 2020 m. gegužės 15 d., žiūrėta gruodžio 1 d., https://lrv.lt/lt/naujienos/lietuva-po-covid-19-investicijos-kurios-keis-ekonomikos-dnr

[44] Europos Sąjungos Taryba, „Pagrindinių teisių chartija dirbtinio intelekto ir skaitmeninių pokyčių kontekste“ 2020 m. spalio 21 d., žiūrėta 2021 m. gruodžio 1 d., https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/lt/pdf

[45] *Ibid*

[46] „Artificial Intelligence & Human Rights“ *Opportunities & Risks*, 2020 m. lapkričio 15 d., žiūrėta 2021 m. gruodžio 1 d., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344

ir DI, gali sustiprinti pagrindinių teisių ir demokratijos apsaugą. Skaitmeninių technologijų pagalba suteikiamas platesnis spektras viešosioms paslaugoms, jos tampa lengviau prieinamos, ekonomiškesnės, DI gali palengvinti pagrindinių teisių apsaugos ir jų pažeidimų dokumentavimą, galima pasitelkti DI hibridinėms grėsmėms identifikuoti ir kovoti su jomis.

Ekspertai teigia, kad tinkamai naudojant DI būtų galima pasiekti ir efektyvesnių teisėsaugos institucijų darbo rezultatų.[47] Vis daugiau finansinių, žmogiškųjų, intelektinių resursų investuojama į DI vystymą lengvinant teisėsaugos institucijų atliekamas užduotis, tai padėtų užtikrinti visuomenės saugumą nacionaliniu ir ES lygmenimis. Atkreiptinas dėmesys, kad pagrindinės sritys, kurios kelia ypatingą susidomėjimą DI sistemų teisėsaugoje naudojimo požiūriu, yra duomenų analizė sistemos, taip pat naujų anksčiau nežinomų modelių bei jų sąsajų interpretavimas.[48] Vis labiau įgalinant DI pagrindu sukurtas sistemas teisėsaugos institucijų veikloje, turi būti užtikrinamos duomenų apsaugos taisyklės ir kitų teisinių bei etikos normų apsauga, taip pat turi būti įtvirtintos atitinkamos apsaugos priemonės. Tiek privačios įmonės, tiek viešojo sektoriaus organizacijos vis dažniau naudoja asmens duomenis mėgindamos suprasti bei nuspėti įvairių žmonių grupių elgseną ir imtis tikslingų priemonių užkardyti tam tikrų asmenų veiklą.

Su intensyviu DI naudojimu teisėsaugos institucijose susijęs tinkamas įvairių rizikų atpažinimas bei vertinimas, tai yra privalomos ir tobulėjant DI sistemoms būtinos apsaugos priemonės, ypač aktualios kalbant apie tokias technologijas kaip masinio stebėjimo priemonės, veido atpažinimo sistemos. Galima pabrėžti, kad vyksta diskusijos apie tai, ar tokios sistemos iš esmės gali būti naudojamos, taip pat analizuojami galimi draudimai jas naudoti. Tikėtina, jog šios sistemos ateityje bus neatsiejama teisėsaugos institucijų veiklos dalis, todėl būtina iš anksto suformuluoti aiškius teisinius reikalavimus jų naudojimui. Visų pirma, naudojant DI turi būti gerbiamos numatytos fundamentinės asmenų teisės ir laisvės, taip pat užtikrinama, kad būtų laikomasi duomenų apsaugos bei privatumą reglamentuojančių teisės aktų ir būtų taikomos veiksmingos teisių gynimo priemonės.[49]

DI technologijų naudojimas yra opus klausimas, kai interneto platformos ir paieškos sistemos, gautą informaciją renka, iš gautų atrenka reikiamą turinį ir nustato DI prioritetus internetinėms svetainėms. Tokiais atvejais, atsiranda pavojus galimybei laisvai

[47] Europos Sąjungos Taryba, „Pagrindinių teisių chartija dirbtinio intelekto ir skaitmeninių pokyčių kontekste“ *supra note,* 8

[48] Donatas Murauskas „Dirbtinio intelekto metodai teisės taikymo srityje – galimybes varžo etiniai klausimai“ *Vilniaus universiteto „Spektrum“,* 2019 lapkričio 11 d., žiūrėta 2021 m. gruodžio 1 d., https://naujienos.vu.lt/dirbtinio-intelekto-metodai-teises-taikymo-srityje-galimybes-varzo-etiniai-klausimai/

[49] Europos Sąjungos Taryba, „Pagrindinių teisių chartija dirbtinio intelekto ir skaitmeninių pokyčių kontekste“ *op. cit.,* 7-8

susipažinti su surinktais informacijos šaltiniais.[50] Būtina kovoti su netinkamu turiniu internete, įskaitant neapykantos nusikaltimus, tuo pačiu apsaugoti ir teisę į saviraiškos laisvę, teisę į informaciją. Reikia pabrėžti, kad labai svarbu, kokiomis aplinkybėmis ir kokia apimtimi naudojant DI sistemos gautus rezultatus norima daryti poveikį konkrečiam turiniui. Tokiu atveju DI sistemos veikia tik esant tikslingam žmogaus įsikišimui.

DI algoritmais ir sistemomis pagrįstos technologijos yra palankiai vertinamos Europos komisijos komunikate Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui[51] rašte, kuriame rašoma, kad „DI grindžiamų inovacijų skatinimas yra glaudžiai susijęs su Europos duomenų strategijos, įskaitant neseniai pateiktą duomenų valdymo aktą, realizavimu“[52], nes DI galima sėkmingai plėtoti tik jei yra užtikrinta sklandi prieiga prie duomenų.[53] Didele rizika, kalbat apie DI sistemos duomenų prieinamumą, yra įvardijamos DI sistemos, kurias ketinama naudoti žmonių įdarbinimo, jų kreditingumo vertinimo ar teismo sprendimų priėmimo tikslais[54]. Todėl taip pat numatoma, jog didelės rizikos DI sistemos turi atitikti tam tikrus specialius reikalavimus, kurie turi būti nustatyti itin svarbių duomenų rinkimui ir jų saugojimui.

Iš pateiktos informacijos, galima daryti išvadą, jog DI turi būti apsaugotas nuo galimo išorės poveikio, o taikant DI būtina užtikrinti asmens teisės bei laisves. ES ekonomine ir reguliuojamąja galia pagrįsti bendri veiksmai plėtojant DI pagrindu veikiančias sistemas, koordinavimo veikla ir bendros investicijos gali turėti didžiulį potencialą Europos pramonei, konkurenciniam pranašumui, stiprinti vidaus rinką bei užtikrinti saugumą. Be to, ES nustatyti patikimumo DI standartai, kaip geroji praktika, gali būti taikomi ir visame pasaulyje, tokiu atveju DI sistemos būtų kuriamos, taip pat įsisavinamos ir prieinamos rinkai, įskaitant teisėsaugos institucijas, atsižvelgiant į ES saugomas vertybes, principus ir teisinį reguliavimą.

---

[50] Swatilekha Chakraborty, Rishabh Bhojwani „Artifical intelligence and human rights: Are they convergent parallel to each other? Protesta“ 2018 m. gruodžio 22 d., žiūrėta 2021 m. gruodžio 1 d., https://repository.ucatolica.edu.co/jspui/bitstream/10983/16334/1/Artificial%20intelligence%20and%20human%20right.pdf

[51] Europos Sąjungos Taryba, „Komisija komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ *op cit.,* 16-18

[52] Europos Komisija, „Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl Europos duomenų valdymo, duomenų valdymo aktas“, *Publications Office of the European Union,* 767 galutinis, 2020 m. lapkričio 25 d., žiūrėta 2021 m. gruodžio 1 d., https://beta.op.europa.eu/en/publication-detail/-/publication/af8cb47b-2f13-11eb-b27b-01aa75ed71a1/language-lt/format-PDF

[53] Europos Sąjungos Taryba, „Komisija komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ *op. cit., 16-18*

[54] *Ibid*

2. DIRBTINIO INTELEKTO TAIKYMAS TEISĖSAUGOS INSTITUCIJOSE

2.1. Dirbtino intelekto ir jo pagrindu sukurtos sistemos teisėsaugos institucijose.

Teisėsaugos institucijų veikla pirmiausiai vertintina vadovaujantis padalijimo principu. Reikėtų įvertinti ne tiek pačias teisėsaugos institucijas, tačiau jų vykdomas funkcijas, kuriomis siekiama įgyvendinti šioms institucijoms keliamus uždavinius.[55] Autoriai, nagrinėjantys teisėsaugos funkcijų problematiką, pripažįsta, jog teisėsaugos institucijų funkcijų ir tarpusavio sąveikos klausimai yra vieni iš svarbiausių užtikrinant teisėsaugos veiklos veiksmingumą.[56] Visos teisėsaugos institucijos, atsižvelgdamos į joms keliamus tikslus ir uždavinius, atlieka teisėsaugos veiklą, atsiskleidžiančią per vykdomas funkcijas.[57] Lietuvoje teisėsaugos institucijos yra įgaliotos įgyvendinti teisę, taip pat yra numatyta, jog privaloma atlikti konkrečias, kiekvienai jų būdingas veiklas, reglamentuotas atitinkamuose norminiuose aktuose.[58] Todėl teisėsaugos funkcijomis turėtume vadinti veiklą įgyvendinant teisės normas, ginant ir saugant žmogaus teises bei vykdant teisingumą, konsultuojant, atstovaujant, o esant būtinybei – ir atliekant gynybos funkcijas.

[59] Šios paminėtos funkcijos nurodo, kad teisėsaugos institucijos yra priverstos neatsilikti nuo šiuolaikinių tendencijų ir dėti visas pastangas, kad funkcijos būtų įgyvendinamos ir užduotys būtų atliekamos per kuo trumpesnį laiką ir kuo efektyviau. Atliekamų funkcijų kokybės gerinimui pritaikomos teisėsaugos institucijoms sukurtos DI programos, kurių tikslas – padidinti teisėsaugos institucijų veiklos efektyvumą.

Teisėsaugos institucijos turėtų būti pajėgios veikti greitai kintančioje nusikalstamoje aplinkoje, kad galėtų sustiprinti visų asmenų apsaugą ir saugumą.[60] DI pagrindu sukurtos programos gali užtikrinti kibernetinį saugumą padėdamos rinkti žvalgybinio pobūdžio

---

[55] Evaldas Visockas, „Pasitikėjimas teisėsaugos institucijomis Lietuvoje“ *Teisės problemos,* 2/2 (2016): 93-107, žiūrėta 2021 m. gruodžio 1 d., https://teise.org/wp-content/uploads/2017/02/Visockas-2016-2.pdf

[56] Pranas Kuconis ir Vytautas Nekrošius, „Teisėsaugos institucijos“ 2001, žiūrėta 2021 m. lapkričio 2 d.,

[57] Malcolm Davies. Hazel Croall, Jame Tyrer, „An Introduction to the Criminal Justice System in England and Wales. Pearson Education“, *Ursula Smartt* 1/1 (2006): 62-71 žiūrėta 2021 m. gruodžio 1 d., https://books.google.lt/books?id=X4j2iLrstToC&pg=PA32&dq=Davies+M.;+Croall,+H.;+Tyrer,+J.+Criminal+Justice+%E2%80%93+An+Introduction+to+the+Criminal+Justice+System+in+England+and+Wales.+Pearson+Education,+2005.&hl=lt&sa=X&ved=2ahUKEwiTtZrCgMv0AhVSQfEDHUNCBo4Q6AF6BAgKEAI#v=onepage&q&f=false

[58] *Ibid*

[59] Gintautas Danišauskas, „Teisėsaugos funkcijų vykdančių institucijų rūšys bei teismo vieta šių institucijų sistemoje“ ISSN 2029–2244, (2009) 2-14, žiūrėta 2021 m. gruodžio 1 d., https://ojs.mruni.eu/ojs/societal-studies/article/download/1415/1356

[60]Europos Komisija „Priedas prie Komisijos komunikato Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui Europos požiūrio į dirbtinį intelektą formavimas“ *EUR-Lex,* 2018 m. balandžio 25 d., 237 galutinis, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2018:237:FIN

informaciją apie galimas grėsmes, analizuodamos ankstesnę patirtį ir atpažindamos tam tikras tendencijas dėl galimų rizikų ir grėsmių. Taip pat DI sistemų pagalba atsiranda galimybė sumažinti reagavimo į iškvietimus laiką, be to, gali būti sudaromos geresnės sąlygos įvairiems iškvietimams išaiškinti laikantis geriausio saugumo praktikos.

ES valstybės narės vidaus reikalų srityje vis dažniau naudoja DI sistemas, kurios įrodė, kad yra naudingos gerinant įvairaus pobūdžio nusikaltimų tyrimą bei užtikrinant viešąją tvarką, padedant pareigūnams tiksliau priimti sprendimus, kovoti su terorizmu.[61] Kuriant ir diegiant DI technologijas teisėsaugos institucijose bei vidaus reikalų srityje yra būtinas tvirtesnis bendradarbiavimas tarp ES valstybių. Suvienijus jėgas ir visapusiškai laikantis pagrindinių žmogaus teisių apsaugos standartų, teisėsaugos institucijos ir kitos vykdančiosios institucijos gali veiksmingai spręsti naujus uždavinius, kurie atsiranda dėl didžiulio apdorojimui reikalingo duomenų kiekio, taip pat atsirandant dar rafinuotesnėms ir sudėtingesnėms nusikalstamoms veikoms. Teisėsaugos institucijose bei organizacijose DI vertinamas visų pirma kaip įrankis užkirsti kelią kibernetiniams nusikaltimams.[62] Įgyvendinant DI sistemų taikomas programas, atsiranda reikalavimai taikyti sklandžias, greitas, patogias skaitmenines sistemas. Todėl ES valstybės narės kaip vieną iš politinių prioritetų įvardijo svarbų etapą: būtinumą remti laisvės, saugumo ir teisingumo erdvės veikimą, kad teisėsaugos institucijos galėtų naudoti DI savo kasdieniame darbe, taikydamos aiškias apsaugos priemones.[63] ES valstybės narės paragino Europos Komisiją skatinti sukurti DI sistemų rezervą ir padėti sukurti teisėsaugos institucijoms skirtas skaitmeninio raštingumo ir įgūdžių mokymo galimybes.[64]

2020 m. gruodžio 9 d. Komisija priėmė ES kovos su terorizmu darbotvarkę[65], kurioje pabrėžiamas gilus DI poveikis teisėsaugos institucijų gebėjimui reaguoti į terorizmo grėsmes, laikantis pagrindinių teisių ir laisvių apsaugos įpareigojimų. Be to, ES valstybės narės įsteigė ES vidaus saugumo inovacijų centrą, kuris taip pat daug dėmesio skiria DI priemonių kūrimui[66] ir atlieka bendradarbiavimo su kitomis valstybėmis funkciją. Pasak ES komisijos, vidaus augumo centras visų pirma įgalins ES policijos (*Europolo*), sienos apsaugos pajėgų (*Frontex*) ir vidaus

[61] Europos Komisija „Priedas prie Komisijos komunikato Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui Europos požiūrio į dirbtinį intelektą formavimas“ *supra note,* 2

[62] Vincenzo Ciancaglini, Craig Gibson, ir David Sacho, „Malicious Uses and Abuses of Artificial Intelligence“ UNICRI Trend Micro, 2020 m. lapkričio 19 d., žiūrėta 2021 m. gruodžio 1 d., https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence

[63] Europos Sąjungos Taryba „Tarybos išvados dėl vidaus saugumo ir Europos policijos partnerystės“ 2020 m. lapkričio 24 d., žiūrėta gruodžio 1 d., https://www.consilium.europa.eu/lt/press/press-releases/2020/12/14/internal-security-council-adopts-conclusions-to-strengthen-cooperation/

[64] *Ibid*

[65] Europos Komisija „Komisijos komunikatas dėl ES saugumo sąjungos strategijos“, *EUR-Lex,* 2020 m. liepos 24 d., 605 galutinis, žiūrėta gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020DC0605

[66] *Ibid*

reikalų IT sistemų agentūrų („*eu-LISA*“) veiklos koordinavimo mechanizmą.[67] Centro tikslas - padėti teisėsaugos institucijoms dalintis informacija bei turimomis žiniomis, taip pat rengti bendrus projektus ir skleisti rezultatus, sukurtus technologinių sprendinių. Europos Komisija pateikė pasiūlymą dėl sustiprintų Europolo įgaliojimų naudojant DI technologijas, kurias naudodama agentūra galėtų kovoti su besiformuojančiomis kibernetinėmis grėsmėmis. Dėl šių įgaliojimų įgyvendinimo yra sudarytos sąlygos veiksmingai bendradarbiauti su teisėsaugos institucijomis, sustiprintas Europolo vaidmuo inovacijų srityje.[68] Europolas turėtų atlikti itin svarbų vaidmenį:

1) padėdamas valstybėms narėms kurti naujus DI grindžiamus technologinius sprendimus, kurie būtų naudingi nacionalinėms teisėsaugos institucijoms visoje ES.[69]

2) populiarindamas etišką, patikimą ir į žmogų orientuotą DI technologijų veiklą, kuriai taikomos griežtos saugumo, saugos ir pagrindinių teisių apsaugos priemonės.[70]

Taip pat gerai žinoma, kad nusikalstamos grupuotės nevengia naudoti DI programas kaip atskiras veikas atlikti įvairaus pobūdžio nusikaltimams. Teisėsaugos institucijos yra neatsiejamos nuo robotizuotų technologijų, tai vienas iš esminių DI įgyvendinimo elementų.[71]

DI paremtos sistemos ir programos yra ganėtinai nauja teisėsaugos veiklos sritis. Lietuvoje daugelis teisėsaugos institucijų jau aktyviai tiria DI taikymą ir galimybę įtraukti robotus atliekant tam tikras funkcijas, siekiant sustiprinti nusikalstamumo prevenciją ir kontrolę. Platus DI programų naudojimo spektras yra kuriamas laikantis nacionalinių nusikalstamumo užkardymo prioritetų. Teisėsaugos institucijų ir DI santykis nėra vienareikšmis. Kai kurios šalys yra labiau pažengusios nei kitos, vertinant šių DI technologijų naudojimą[72]. DI sistemos bei technologijos, naudojamos visose šiose Lietuvos teisėsaugos institucijose:

- Policijos departamentas prie Vidaus reikalų ministerijos,
- Valstybės sienos apsaugos tarnyba prie Vidaus reikalų ministerijos,
- Kalėjimų departamentas prie Lietuvos Respublikos teisingumo ministerijos,

---

[67] Europos Komisija „Priedas prie Komisijos komunikato Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui Europos požiūrio į dirbtinį intelektą formavimas“ *supra note, 3*

[68] Europos Komisija „Europos Parlamento ir Tarybos reglamentas, kuriuo dėl Europolo bendradarbiavimo su privačiais subjektais, Europolo atliekamo asmens duomenų tvarkymo padedant atlikti nusikalstamų veikų tyrimus ir Europolo vaidmens mokslinių tyrimų ir inovacijų srityje iš dalies keičiamas Reglamentas“ *EUR-Lex,* 2020 m. gruodžio 9 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52020PC0796&from=LT

[69] Europos komisija „Komisijos komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ *EUR-Lex,* 2021 m. balandžio 22 d., 205 galutinis, žiūrėta 2021 m. gruodžio 1 d., https://data.consilium.europa.eu/doc/document/ST-8334-2021-INIT/lt/pdf

[70] *Ibid*

[71] Europos Komisija „Komisijos komunikatas dėl ES saugumo sąjungos strategijos“, *supra note,* 3.

[72] „What is artificial intelligence and how is it used?“ *Europen Parliament News,* 2021 m. kovo 29 d., žiūrėta gruodžio 1 d., https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

- Viešojo saugumo tarnyba prie Vidaus reikalų ministerijos,
- Vadovybės apsaugos tarnyba,
- Muitinės departamentas prie Finansų ministerijos
- Teisingumo ministerija
- Krašto apsaugos ministerija

Įgyvendinant šių teisėsaugos institucijų kompetencijas naudojamos DI modelio sukurtos programos bei algoritmai.[73] Teisėsaugos funkcijas atliekančios institucijos turi skirtingo pobūdžio sistemas, kurių viena iš sudedamųjų dalių yra DI algoritmai.[74] Šiame darbe aptarsime keletą svarbiausių teisėsaugos institucijų ir jų naudojamų DI programų bei algoritmų funkcijų. Šios teisėsaugos institucijos yra Policijos departamentas, Valstybės sienos apsaugos tarnyba, Teisingumo ministerija.

2.2. Dirbtinio intelekto ir jo pagrindu sukurtos sistemos policijos institucijose

DI pamažu, bet užtikrintai tampa priemone užkardyti, sustabdyti nusikaltėlius bei analizuoti atliekamus neteisėtus veiksmus. Daugelis teisėsaugos institucijų visame pasaulyje naudoja naujausias technologijas, kad užkirstų kelią nusikalstamumui. Vienas iš tokių sprendimų yra veido atpažinimo sistemos, kurias plačiai taiko įvairiuose sektoriuose siekiant užtikrinti saugumą. Policijos veikloje naudojamos plataus spektro DI sistemos, kurios atlieka analizę kompiuterių pagalba.[75]

DI kaip technologija policijoje dažniausiai naudojama vaizdo atpažinimo kamerų pavidalu. Šių kamerų viena iš pagrindinių funkcijų yra didelės minios stebėjimas, identifikuojant nestandartinį ar neadekvatų asmenų elgesį. Vaizdo kamerų pagalba galima įvertinti pateiktą filmuotą medžiagą bei optimaliai pritaikyti veido atpažinimo sistemą. Taip pat atliekant viešą stebėjimą galima užfiksuoti tam tikrus pažeidimus bei atlikti prevencijos funkciją. Tikimasi, kad DI policijoje sustiprins visuomenės saugumą.

Dar viena svarbiausių policijos funkcijų, kurią galima atlikti pasitelkiant DI, yra sukčiavimo nusikaltimų atpažinimas, eismo įvykių ar netinkamo elgesio viešoje erdvėje analizė.

---

[73] Europos Komisija, „Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology“ *Europos Sąjungos leidinių biuras Ecorys*, 2021 m. vasario 15 d., žiūrėta 2021 m. gruodžio 1 d., https://op.europa.eu/lt/publication-detail/-/publication/5afa29f0-700a-11eb-9ac9-01aa75ed71a1/language-en/format-PDF/source-191372680

[74] *Ibid*

[75] „How Artificial Intelligence In Policing Helps Crime Detection“ *INNEFU*, 2021 m. vasario 1 d., žiūrėta 2021 m. gruodžio 1 d., https://www.innefu.com/blog/how-artificial-intelligence-in-policing-helps-crime-detection

DI turi didelį potencialą taikant atpažinimo funkcijas šiose srityse.[76] Šių priemonių naudojimas teisėsaugoje trumpina tyrimo laiką, taip pat eliminuoja žmogiškąsias klaidas bei žmogiškojo nuovargio elementą.[77] Šių priemonių naudojimas mažina institucijų žmogiškųjų resursų poreikį ir yra ekonomiškas, kadangi nereikia fizinio pareigūno atliekant tokias funkcijas. DI yra pagrįstas algoritmais, o plečiantis šių sistemų naudojimui atsiranda didesnė informacinė duomenų bazė apie tam tikrus nusikaltimus.[78] Perspektyviausias DI pritaikymas teisėsaugai yra gebėjimas nustatyti bei išaiškinti potencialiai pavojingas veikas, taigi atsiranda galimybė geriau numatyti ir užkirsti kelią nusikaltimams. Šis gebėjimas, numatyti nusikalstamas veikas prieš joms įvykstant, yra žinomas kaip nuspėjamoji policija (*angl. predictive policing*).[79]

Nuspėjamojoje policijoje DI algoritmai naudojami siekiant nustatyti ir surūšiuoti didelius kiekius gautų duomenų apie įvairią veiklą, DI algoritmas gali būti naudojamas ir siekiant nustatyti žmones, kurie gali kelti pavojų. Tokie procesai yra žinomi kaip rizikos ar galimos grėsmės vertinimas. Svarbu pažymėti, kad surinkti istoriniai duomenys, kuriais remiamasi kuriant algoritmus, kelia didelį susirūpinimą dėl duomenų autentiškumo. Visų pirma, pateikti duomenys gali būti klaidingi, kadangi teisėsaugos pareigūnai gali neteisingai juos įvesti į algoritmų sistemą, ypač dėl to, kad nusikalstamos veikos duomenys dažniausiai yra daliniai ir netinkami naudojimui.[80] Pateikti duomenys gali būti neišsamūs ir tam tikru atveju šališki, kadangi nusikaltimų požymiai labai retai sutampa ir yra šabloniški. Taip pat gali kilti netikslumų dėl įvestų į sistemą duomenų, nes pareigūnai galimai gali vykdyti diskriminacinę veiklą prieš tam tikras bendruomenes, neteisingai priskirdami su tokiais asmenimis susijusias veikas prie „didelės rizikos“ vertinimo“.[81] Pavyzdžiui, tam tikroje situacijoje policijos pareigūnai, dirbantys su DI sistemomis, pritaiko didesnės rizikos faktorių juodaodžių žmonių atžvilgiu. Dėl to šis numanomų istorinių duomenų, įvestų į algoritmus, šališkumas turi milžiniškų pasekmių tam

[76] Gonzalez Fuster, „AI and law enforcement: Impact on fundamental rights“, *European Parliament ThinkTank,* 2020 m. liepos 7 d., žiūrėta 2021 m. gruodžio 1 d., https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf,
[77] Rayn Jenkins ir Duncan Purves „Artificial Intelligence and Predictive Policing: A Roadmap for Research“ *Ethics+Emerging Sienses Group,* 2020 m. rugsėjo 30 d., žiūrėta 2021 m. gruodžio 1 d., http://aipolicing.org/year-1-report.pdf,
[78] Cynthia Rudin, „Predictive Policing: Using Machine Learning to Detect Patterns of Crime“, *Wired,* 2021 m. liepos 2 d., žiūrėta 2021 m. gruodžio 1 d., https://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime/
[79]Christopher Rigano, „Using Artificial Intelligence to Address Criminal Justice Needs“ *National Institute of Justice Journal,* 2019 m. sausio 17 d., žiūrėta 2021 m. gruodžio 1 d., https://www.ojp.gov/pdffiles1/nij/252038.pdf
[80] Matthias Leese, „Predictive Policing: Proceed, but with Care“, *Policy Perspectives* 2020 m. gruodžio 6 d., žiūrėta 2021 m. gruodžio 1 d., https://www.researchgate.net/publication/347443927_Predictive_Policing_Proceed_but_with_Care
[81] „Now Human Rights in the Age of Artificial Intelligence“, *Accessnow,* 2018 m. lapkričio 2 d., žiūrėta 2021 m. gruodžio 1 d., https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf,

tikroms bendruomenėms.[82] Dėl to DI naudojimas nuspėjamojoje policijos veikloje gali nulemti analizės šališkumą, todėl tai galima vadinti rasistiniu profiliavimu, pavyzdžiui, Brisha Borden ir Vernon Parter atvejai. Borden atveju, 18 metų juodaodė mergina, neturėjusi jokių ankstesnių nusižengimų, ir, Vernonas Parteris, 41 metų baltaodis vyras, anksčiau kaltintas ginkluotu apiplėšimu ir nuteistas 5 metams kalėjimo, buvo apkaltinti įvairiomis prekių iš parduotuvių vagystėmis 2014 m. Tačiau DI algoritmas „COMPAS“ (verčiamas kaip „Pataisos pažeidėjo valdymo profiliavimas alternatyviomis sankcijoms“), kurį JAV policijos departamentai naudojo rizikos vertinimui atlikti, nustatė, jog būtent Borden, kaip galimai yra didelės rizikos zonoje, ir ateityje gali būti nuteista, o Parteriui buvo priskirta žemiausio lygio rizika atlikti nusikaltimus. DI algoritmas aiškiai diskriminavo Borden dėl jos rasės.[83]

Be to, sistemoje naudojami duomenys dažnai yra nukreipiami į nusikaltimų gatvėse užkardymą, o tokios nusikalstamos veikos, kaip vagystės ar prekyba narkotikais dažniausiai siejamos su tam tikromis demografinėmis grupėmis ir gyvenamaisiais rajonais. Tačiau interaktyviems nusikaltimams, tokiems kaip pinigų plovimas, įmonių sukčiavimas ar mokesčių slėpimas, skiriama mažiau dėmesio. Taip pat tokie duomenys, kaip informacija apie galimą smurtą artimoje aplinkoje, iš esmės nėra analizuojama ir nėra žinoma, apie šioms veikoms užkardyti naudojamas DI sistemas.[84] Toks nuspėjamosios policijos atrankos šališkumas yra identifikuojamas informacinėse sistemos, todėl pateikti duomenys niekada neturėtų būti laikomi tinkamais konkrečiam sprendimui priimti.[85]

Taigi DI naudojimas nuspėjamojoje policijos veikloje palengvina tai, kas, pasak Peter M. Asaro, vadinama „probleminiu nusikalstamumo tipu.“[86] Remiantis algoritmuose įvesta informacija, kai kurie šalių rajonai ar tam tikri asmenys gali sulaukti padidintos stebėsenos iš teisėsaugos pusės, pavyzdžiui, dažniau tikrinant asmenų tapatybę patruliuojant. Dėl šių veiksnių gali pablogėti esami santykiai ir sumažėti pasitikėjimas tarp gyventojų ir policijos. Taip pat didelį susirūpinimą kelia ir DI sistemų veikimo ir procesinių sprendimų priėmimo skaidrumo trūkumas. UNICRI ir Interpolo bendroje ataskaitoje numatyta, jog DI sprendimai ir veiksmai

[82] Peter M. Asaro, „AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care“ *IEEE Technology and Society Magazine*, 2019 m. rugsėjo 28 d., žiūrėta 2021 m. gruodžio 1 d., https://ieeexplore.ieee.org/document/8733937

[83] „Artificial Intelligence Predictive Policing: Efficient, or Unfair“ *Security Distillery.*, 2021 m. liepos 23 d., žiūrėta 2021 m. gruodžio 1 d., https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing

[84] Julia Angwin, Jetf Larson, Surya Mattu ir Lauren Kirchner, „Machine Bias“ *ProPublica*, 2016 m. gegužės 23 d., žiūrėta 2021 m. gruodžio 1 d., https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[85] Matthias Leese, „Predictive Policing: Proceed, but with Care“, *Policy Perspectives* 2020 m. gruodžio 6 d., žiūrėta 2021 m. gruodžio 1 d., https://www.researchgate.net/publication/347443927_Predictive_Policing_Proceed_but_with_Care

[86] M. Asaro op. cit.

visada turi būti suprantami įvairių pusių naudotojams, DI privalo gerbti pagrindines piliečių teises.[87]

DI algoritmai gali būti naudojami atliekant nuspėjamosios policijos funkcijas, kurie dėl didelio informacijos kiekio gali būti labai sudėtingi ir netikslūs, kadangi kiekvieną įvestą sisteminę informaciją reikia nuolat atnaujinti.[88] DI sistemų veiklos skaidrumo trūkumas lemia tam tikros atsakomybės bei įvertinimo netikslumus. Esant dabartinei situacijai DI panaudojimui nuspėjamojoje policijoje reikia tinkamo teisinio reguliavimo, kad būtų išvengta didėjančios socialinės nelygybės ir padidintų pasitikėjimą teisėsaugos ir teismų sistema.[89]

Europoje taip pat yra taikoma viena iš DI sistemų recidyvizmo rizikos nustatymo priemonė. Ši teisinės priemonės sistema vadinama „HART“. Šią sistemą naudoja Jungtinė Karalystė, kurioje vystoma šios valstybės teisėsaugos institucijų ir Kembridžo universitetų mokslininkų sukurta bei tobulinama sistema. Ji analogiškai atpažįsta ir nustato recidyvizmą taip pat, kaip ir JAV naudojama programa, kuomet tikslinga nustatyti pakartotinio asmens nusikaltimo riziką. Šioje programoje taip pat vertinami kriterijai, kurie gaunami asmeniui atsakius į tam tikrus klausimus, atsižvelgiama ir į policijos pateiktus duomenis apie minėtą asmenį.[90]

2.3. Dirbtino intelekto ir jo pagrindu sukurtų sistemų taikymas Valstybės sienos apsaugos tarnyboje

DI sistemų taikymas Valstybės sienos apsaugos tarnyboje (toliau – VSAT) nėra naujovė, kiekvienais metais šios technologijos yra tobulinamos. VSAT naudoja įvairaus tipo technines programas, kurios veikia pasitelkdamos sukurtus DI sistemų algoritmus. Literatūroje daugiausiai informacijos pateikiama apie pažeidimų identifikavimo technologijas. Šios technologijos yra sumontuotos kontroliniuose valstybės sienos postuose. Fizinė valstybės sienos apsauga dažniausiai yra užtikrinama įvairiais būdais: vandenyse esančiais riboženkliais, kontrolinėmis pėdsakų juostomis, sausumos stulpeliais tiek miškingose vietovėse, tiek pievose,

[87] „Artificial Intelligence and Robotics for Law Enforcement*“, United Nations Interregional Crime and Justice Research Institute (UNICRI) and International Criminal Police Organization* (INTERPOL), 1-1 (2019) 23 – 26, žiūrėta 2021 m. gruodžio 1 d., http://www.unicri.it/artificial-intelligence-and-robotics-law-enforcement,
[88] *Ibid*
[89] Europos Komisija, „Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology“ *Europos Sąjungos leidinių biuras Ecorys*, 2021 m. vasario 15 d., žiūrėta 2021 m. gruodžio 1 d., https://op.europa.eu/lt/publication-detail/-/publication/5afa29f0-700a-11eb-9ac9-01aa75ed71a1/language-en/format-PDF/source-191372680
[90] „Artificial Intelligence, Robotics, Privacy and Data Protection“ *International privacy conference*. 2016 m. spalio 5 d., žiūrėta 2021 m. gruodžio 1 d., https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

taip pat įvairaus pobūdžio užtvaromis.[91] Valstybė nuolat stiprina fizinę sienų kontrolę, tačiau kontrolės metodai ir priemonės labai dažnai keičiasi tiek valstybės viduje, tiek už numatytos teritorijos ribų.[92] Valstybės sienų kontrolė yra išplečiama už demarkuotų sienų ribų ir vykdoma naudojant daugybę nuotoliniu būdu valdomų sistemų,[93] pvz., registracija prieš išvykimą iš valstybės, nuotolinis patikrinimas ir skaitmeninis stebėjimas atvykstančių, išvykstančių objektų. Šis stebėjimas gali užtikrinti tvarką, kad nebūtų pažeidžiami numatyti reikalavimai. Sienų apsaugos funkcijas padeda įgyvendinti ir pasienio tarnyboje naudojamos technologijos, skirtos biometrinių duomenų identifikavimui, profiliavimui ir rizikos analizei. Nuotolinis riziką keliančių žmonių atpažinimas, žvelgiant iš istorinės perspektyvos, atsirado visai neseniai, pradėjus VSAT taikyti įvairias technologijas, kurios veikia DI sistemų pagrindu. Ši asmenų, kertančių valstybės sieną, stebėjimo technologija skirta asmenims identifikuoti. Pagrindinis šiuolaikinių valstybių sienų apsaugos poreikis yra identifikuoti asmenis, kurie atvyksta į valstybes.[94] Tokie technologijos taikymai yra pagristi tuo, kad atsiranda galimybė atlikti asmenų, kertančių valstybės sieną, kontrolę bei nustatyti galimus jų neteisėtus tikslus, užtikrinant saugumą nuo terorizmo bei kitų išpuolių atveju.[95] Asmenų identifikavimo problemos tapo ypač aktualios pastaruoju metu nelegalios migracijos kontekste, kai asmenys masiškai pradėjo kirsti valstybių sienas, naudodami suklastotus ar negaliojančius dokumentus.[96] Todėl valstybės sienos apsaugos sistemoje taikoma vis naujų DI technologijų, tai yra skatinama ES lygmenyje, ypač daug dėmesio skiriant saugaus DI sistemų naudojimo užtikrinimui.[97]

Nors galimybių panaudoti DI kaip įrankį sienų apsaugos funkcijų veiksmingumui gerinti yra daug, taip pat yra ir nemažai galimų kliūčių norint jį tinkamai naudoti. Aptarsime keletą problemų, su kuriomis susiduria VSAT naudodama DI technologijas.

Pirma, tokios problemos kaip DI algoritmų skaidrumo stoka ir galimi šališkumai apriboja DI sistemų naudojimą. Naujame ES siūlyme taikant DI technologijas pažymima keletas

---

[91] Nutarimas „Dėl valstybės sienos ženklų, ženklinančių Lietuvos Respublikos sieną sausumoje ir pasienio vandenyse, formos, dydžio nustatymo ir jų statymo tvarkos aprašo patvirtinimo“ *Lietuvos Respublikos vyriausybė, Valstybės žinios,* 2007 m. kovo 21 d. Nr. 44-16, žiūrėta 2021 m. gruodžio 1 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.295850/asr

[92] Ainhoa Ruiz Benedicto, Mark Akkerman, ir Pere Brunet, „A Walled World: Towards a global apartheid” *Report, Transnational Institute,* 2020 m. lapkričio 18 d., žiūrėta 2021 m. gruodžio 1 d., https://www.tni.org/en/walledworld

[93] Arsitide R. Zolberg, „Managing a world on the move”, *Population and Development Review,* 2006 m. liepos 15 d., žiūrėta 2021 m. gruodžio 1 d., https://www.jstor.org/stable/20058950

[94] James C. Scot „How certain schemes to improve the human condition have failed”, *Yale university Press*, 2008 m. vasario 2 d., žiūrėta 2021 m. gruodžio 1 d., https://politicalscience.yale.edu/publications/seeing-state-how-certain-schemes-improve-human-condition-have-failed

[95] Ayelet Shachar, „Borders in the Time of COVID-19”, *Ethics and International Affairs*, 2020 m. kovo 8 d. žiūrėta 2021 m. gruodžio 1 d., https://www.ethicsandinternationalaffairs.org/2020/borders-in-the-time-of-covid-19/

[96] Alexander Todorov „Face value: The irresistible influence of first impressions“, *Princeton University Press,* 2017 m. birželio 6 d., žiūrėta 2021 m. gruodžio 1 d., https://press.princeton.edu/books/hardcover/9780691167497/face-value

[97] Kate Crowford, „Time to regulate AI that interprets human emotions“, *Nature*, 2021 m. balandžio 6 d., žiūrėta 2021 m. gruodžio 1 d., https://www.nature.com/articles/d41586-021-00868-5

iššūkių apibrėžiant pasitikėjimo ir DI ugdymo svarbą, taip pat nurodomi būtini politikos pokyčiai ir investicijos, reikalingos siekiant sustiprinti „į žmogų orientuoto, tvaraus, saugaus, ir patikimo, DI plėtrą.“[98] Patikimo ir visa apimančio DI naudojimas galėtų atlikti ypač svarbų vaidmenį sienų saugumo kontekste. Taip yra todėl, kad DI palaikančių technologijų naudojimas sienų saugumui yra kritikuojamas dėl galimo žmogaus teisių ir su privatumu susijusių apsaugos priemonių pažeidimo.[99] Reikia atlikti išsamų rizikos vertinimą, siekiant užtikrinti, kad technologijų plėtra atitiktų tvarias ES etikos ir žmogaus teisių apsaugos standartų gaires.

Antra, be technologinių kliūčių DI įsisavinimą ES valstybių sienų apsaugoje gali riboti tai, kad visos teisėsaugos institucijos turi dalintis bendra sistemų praktika naudojant DI kaip įrankį. Atsiranda galimi trukdžiai - techninės patirties ir su naujomis technologijomis susijusių įgūdžių trūkumai,[100] dažnai ribojantys viešojo sektoriaus organizacijų gebėjimą atpažinti ir visapusiškai išnaudoti DI technologijų teikiamas galimybes.

Trečia, viena iš problemų taikant DI sienų apsaugai yra tai, jog šias sistemas naudojančios teisėsaugos institucijos yra atsakingos už nacionalinį saugumą, todėl dažnai DI technologijų testavimai atliekami kontroliuojamoje aplinkoje, o tai neleidžia visapusiškai įvertinti technologijų veikimo. Šis DI naudojimo aspektas riboja supratimą apie tai, kokį poveikį DI technologijos iš tikrųjų gali turėti. Šiame kontekste labai svarbi ES agentūrų ir organizacijų, pvz., Europos sienų ir pakrančių apsaugos agentūros (FRONTEX), veikla.[101] Ši agentūra gali suvienyti ir nukreipti mokslinius tyrimus į svarbiausias sritis, orientuotas į žmogaus teisių apsaugą vystant DI sistemas.

2.4. Dirbtinis intelektas ir žmogaus teisės teisėsaugos institucijų veikloje

DI sistemų, algoritmų ar kitų su DI susijusių technologijų veikla dažniausiai siejama su svarbiomis asmens teisėmis į privatų gyvenimą, taip pat asmens garbe, orumu, reputacija. Visas šias išvardytas teises užtikrina tiek LR Konstitucija, tiek Europos žmogaus teisių komisija, tiek ir kiti tarptautiniai dokumentai. Pagal ES pagrindinių teisių chartijos 7 straipsnį visiems asmenims ES yra garantuojama pagarba privačiam ir šeimos gyvenimui, o pagal 8 straipsnį teisė į asmens duomenų apsaugą.[102] Chartijoje reikalaujama, kad tokie duomenys būtų tvarkomi tinkamai ir naudojami tik konkretiems tikslams, užtikrinant kiekvieno asmens teisę susipažinti su asmens

[98] Europos Komisija „Pasiūlymas Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami tam tikri sąjungos teisėkūros procedūros, priimami aktai“ 2021 balandžio 21 d., 206 galutinis, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

[99] *Ibid*

[100] *Ibid*

[101] *Ibid*

[102] Europos Sąjunga „Europos Sąjungos pagrindinių teisių chartija“, *EUR-Lex,* 2016 m. spalio 17 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12016P/TXT&from=LT

duomenimis ir teisę tokius duomenis koreguoti. LR Konstitucijos 22 straipsnio 3 dalyje yra nuostata, jog „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą,“[103] taip pat šio straipsnio 4 dalies nuostata „įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą.“[104] Šios nuostatos yra vienos iš svarbiausių asmens privataus gyvenimo neliečiamybės garantijų. Remiantis jomis yra saugomas asmens privatus gyvenimas nuo valstybės, institucijų, jų pareigūnų, kitų asmenų neteisėto kišimosi.

Aiškinamasi, kiek DI gali šias teises ir laisves pažeisti, ir kiek šių teisių ir laisvių pažeidimai gali būti pateisinami. 2016 m. ES ėmėsi iniciatyvos ir sustiprino minėtų teisių apsaugą, priimdama Bendrąjį duomenų apsaugos reglamentą bei „Direktyvą dėl fizinių asmenų apsaugos duomenų tvarkant asmens duomenis su nusikalstamomis veikomis susijusias arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo.“[105] Teisėsaugos institucijos analizuoja asmens duomenis siekdamos užtikrinti nusikalstamų veikų prevenciją, palengvinti tyrimą bei atskleidimą[106]. DI sistemų pagalba šiuos procesus galima palengvinti ir užtikrinti, kad surinkti duomenys būtų tinkamai išanalizuoti. Bendrojo duomenų apsaugos reglamento taikymas ES gali padidinti pasitikėjimą DI technologijų sistemomis, nes žmonės įgalinami kontroliuoti savo asmens duomenų naudojimą. Kartu yra užtikrinamas laisvas asmens duomenų judėjimas tarp ES valstybių narių.

ES asmens duomenų apsauga tampa viena iš pagrindinių saugomų teisių. Žmogaus teisės, kurios gali būti paveiktos naudojant automatizuotus apdorojimo metodus ir algoritmus:

1. Teisė į teisingą teismo procesą ir tinkamą proceso eigą.
2. Privatumas ir duomenų apsauga.
3. Saviraiškos laisvė.
4. Susirinkimų ir asociacijų laisvė.
5. Teisė į veiksmingą teisių gynimo priemonę.
6. Diskriminacijos draudimas.
7. Socialinės teisės ir galimybė naudotis viešosiomis paslaugomis.

---

[103] „Lietuvos Respublikos Konstitucija“. *Valstybės Žinios*, 1992, Nr. 33-1014, žiūrėta 2021 m. gruodžio 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1890/asr

[104] *Ibid*

[105] Europos Sąjunga „Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas“ 2016 m. balandžio 27 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016L0680&from=LT

[106] Europos Sąjunga, „Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“ 2016 m. balandžio 27 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016R0679&from=LT

8. Teisė į laisvus rinkimus.[107]

Kita vertus, šiuolaikiniame pasaulyje žmonėms plačiai naudojantis įvairiais DI algoritmais, t. y. veikiančiais socialiniais tinklais (Facebook, Twitter, Instagram, Linkedln ir kt.) bei išmaniųjų telefonų bendravimo programomis (Viber, Messenger, Whatsapp ir kt.) žmogaus teisės gali būti pažeidžiamos net patiems asmenims to nežinant, kadangi kiekviena veikianti programa renka informaciją ir ją saugo.[108] Tokia informacija gali būti ir viešai pačių asmenų pateikiami duomenys apie asmeninį gyvenimą. Taigi, teisėsaugos institucijoms tampa įmanoma sekti asmenis ir teisėtai rinkti informaciją apie juos. Nors žmogaus privatus gyvenimas, pasak Konstitucijos ir kitų teisės aktų, yra neliečiamas, šiuo atveju žmogaus teisė į privatumą nėra apsaugota, kadangi asmenys patys savo noru dalinasi tokia informacija. Pagal Konstituciją yra galimybė riboti žmogaus teises ir laisves, taip pat žmogaus teisę į privatumą, jeigu laikomasi šių numatytų sąlygų: tai daroma įstatymu; ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises ir laisves, Konstitucijoje įtvirtintas vertybes.[109] Panašaus požiūrio laikosi ir kitos ES valstybės, kurios siekia, jog asmens teisės ir laisvės būtų užtikrintos tinkamai.

Privataus gyvenimo teisinė samprata gali būti siejama su asmens teisėtais privataus gyvenimo lūkesčiais. Anot R. Merkevičiaus, žmogaus privataus gyvenimo apsaugos ribos baigiasi tada, kai jis savo neteisėtais veiksmais ar kitaip pažeidžia saugomus teisės interesus, taip pat jei daro žalą atskiriems asmenims, visuomenei ar valstybei.[110] Dėl to DI sistemos daro didelį poveikį žmogaus teisėms, kurios yra susijusios su valstybės įsipareigojimais apsaugoti kitų žmonių teises.[111] Didelis duomenų antplūdis pasiekė visas socialines sritis, kurios paremtos algoritmais. Šie algoritmai vis labiau prisitaiko prie šiuolaikinio gyvenimo rutinos.[112]

---

[107] „Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications“ *The Committee of Experts on Internet Intermediaries* 1/1 (2017): 36-48, žiūrėta 2021 m. gruodžio 1 d., https://rm.coe.int/study-hr-dimension-of-automateddata-processing-incl-algorithms/168075b94a

[108] „Discrimination in data-supported decision making” *European Union Agency for Fundamental Rights* (2018) 1/1, 6-8, žiūrėta 2021 m. gruodžio 1 d., https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

[109] „Lietuvos Respublikos Konstitucija“. *Valstybės Žinios*, 1992, Nr. 33-1014, žiūrėta 2021 m. gruodžio 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1890/asr

[110] Remigijus Merkevičius, „Baudžiamajame procese atsitiktinai gautos faktinės informacijos panaudojimas kitame baudžiamajame procese“, *Lietuvos Respublikos Baudžiamajam kodeksui - 10 metų,* žiūrėta 2021 m. gruodžio 1 d., https://www.lituanistika.lt/content/41729

[111] „Committee of Experts on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence” *Council of Europe.* 2019 m. kovo 19 d., žiūrėta 2021 m. gruodžio 1 d., https://www.coe.int/en/web/freedom-expression/-/committee-of-experts-on-human-rights-dimensions-of-automated-data-processing-meets-in-strasbourg-for-the-third-time

[112] *Ibid*

2.4. Asmens teisių ir laisvių apsauga nuo dirbtinio intelekto keliamų pavojų

DI yra viena iš strateginių XXI amžiaus technologijų, kuri duoda didelės naudos, susijusios su procesų veiksmingumu, tikslumu, ekonomiškumu. Be kita ko, DI taikomosios programos pagerino sveikatos priežiūrą, padidino ūkininkavimo veiksmingumą, prisidėjo prie DI klimato kaitos švelninimo ir prisitaikymo prie jos, taip pat pagerino gamybos efektyvumą.[113] Plėtojant DI turi būti gerbiamos vertybės, kuriomis grindžiamos ES vertybės, taip pat labai svarbu atsižvelgti į pamatines teises - žmogaus orumą, asmens laisvę, demokratiją.

Analizuojant tokią pasiūlytą vertybių ir principų sistemą DI srityje, turi būti paminėti ir vieni iš pagrindinių ES teisės aktų, t. y. ES sutartis ir ES pagrindinių teisių chartija. ES sutarties 2 straipsnyje yra įtvirtinta nuostata, kad „Sąjunga yra grindžiama šiomis vertybėmis: pagarba žmogaus orumui, laisve, demokratija, lygybe, teisine valstybe ir pagarba žmogaus teisėms, įskaitant mažumoms priklausančių asmenų teises. Šios vertybės yra bendros visoms valstybėms narėms, visuomenėje, kurioje vyrauja nediskriminavimas, tolerancija, teisingumas, solidarumas ir moterų bei vyrų lygybė.“[114] ES pagrindinių teisių chartijoje yra įtvirtintos ir detaliau apibrėžtos ES sutarties 2 straipsnyje nurodytos teisės bei laisvės.

Šiame kontekste, turi būti paminėti ir Aizeko Azimovo (*angl. Isaac Asimovo*)[115] dėsniai:

1. DI nevalia sužeisti žmogaus ar per savo neveiklumą leisti žmogui patirti skriaudą.
2. DI turi klausyti žmogaus jam duotų nurodymų, nebent jie prieštarautų pirmajam dėsniui.
3. DI turi saugoti savo paties egzistavimą, nebent toks saugojimas prieštarautų pirmajam ir antrajam dėsniui.[116]

Šiuos dėsnius „reikia traktuoti kaip taikytinus DI intelektinėms sistemoms, įskaitant robotus, turinčius integruotą autonominio veikimo ir savarankiško mokymosi režimą, kūrėjams, gamintojams ir operatoriams, kadangi šių dėsnių negalima paversti mašininiu kodu.“[117]

Taigi toliau bus aptartos svarbiausios asmenų teisės bei laisvės apsaugos nuo galimų DI sistemų disfunkcijų kontekste.

---

[113] Europos Parlamentas „Pasiūlymas Dėl dirbtinio intelekto baudžiamojoje teisėje ir jo naudojimo policijoje ir teisminėse institucijose baudžiamosiose bylose“ žiūrėta 2021 m. gruodžio 1 d., https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_LT.pdf

[114] „Europos Sąjungos sutarties suvestinė redakcija“, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12012E/TXT&from=LT

[115] Isaac Asimov — JAV rašytojas fantastikas, mokslo populiarintojas, pagal profesiją biochemikas. Apsakyme „Robis“ suformavo 3 dėsnius, tapusius robotų moralės kodeksu taikomu iki pat šių dienų. https://lt.wikipedia.org/wiki/Isaac_Asimov

[116] Greg Hullender „Asimov's Centennial: Eight Stories September 1941-April 1943“ *Featured Futures,* https://featuredfutures.wordpress.com/2020/02/10/asimovs-centennial-eight-stories-september-1941-april-1943/

[117] Europos Parlamentas „Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų“ žiūrėta 2021 m. gruodžio 1 d., https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_LT.html

Pirmiausia, reikėtų aptarti vieną iš svarbiausią asmens teisių - teisę į duomenų apsaugą, kadangi šiuo metu pagrindinis internetinio verslo modelis yra glaudžiai susijęs su didelio masto stebėjimu, kas, kai kurių autorių nuomone, kelia grėsmę visuomenės saugumui ir jų duomenų stebėjimu, kas , kai kurių autorių nuomone, kelia grėsmę visuomenės saugumui ir jų duomenų apsaugai.[118] Ryškiausias pastarųjų metų pavyzdys yra *Facebook* socialinis tinklas, kuris stebi žmonių veiklą pasitelkiant internetą, netgi jeigu jie nėra *Facebook* nariai. Tikėtina, kad Facebook pasidalino su trečiosiomis šalimis savo vartotojų (~ 87 mln. paskyrų) duomenimis be jų žinios ir sutikimo, tokiais veiksmais pažeidžiant vartotojų teisę į duomenų apsaugą. Toks stebėjimas gali atskleisti ir pažeisti pačią jautriausią informaciją apie asmenis, t. y. nuo tokių paprasčiausių duomenų, kaip vardas, pavardė, elektroninis paštas, telefono numeris ir kt. iki informacijos apie asmens tautybę, rasę, seksualinę orientaciją, politines pažiūras, socialinę padėtį, sveikatą, biometrinius duomenis ir kt. Analizuojant asmens teisę į duomenų apsaugą, reikia paminėti toliau nagrinėjamus teisės aktus, t. y. Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[119], taip pat 2016 m. įtvirtintą ES pagrindinių teisių chartiją. Tartis dėl ES veikimo su Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva[120].

Taip pat labai svarbus ES pagrindinių teisių chartijos 8 straipsnis, kuriame yra įtvirtinta asmens duomenų apsauga.

8 straipsnis. Asmens duomenų apsauga

1. Kiekvienas turi teisę į savo asmens duomenų apsaugą.[121]
2. Tokie duomenys turi būti tinkamai tvarkomi ir naudojami tik konkretiems tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais. Kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei į tai, kad jie būtų ištaisomi.
3. Nepriklausoma institucija kontroliuoja, kaip laikomasi šių taisyklių.

Šis teisės aktas yra laikomas pamatiniu ES teisės aktu, nustatančiu saugomas teises bei laisves. Pažymėtina, kad Sutartyje dėl ES veikimo 16 straipsnyje taip pat yra įtvirtinta teisė į

[118] Bruce Schneier, „The Public-Private Suveillance Partnership“, *The Atlantic*, 2013 m. lapkričio 8 d., žiūrėta 2021 m. gruodžio 1 d. https://www.theatlantic.com/technology/archive/2013/11/a-fraying-of-the-public-private-surveillance-partnership/281289/

[119] Europos Komisija „Pasiūlymas Tarybos sprendimas kuriuo, atsižvelgiant į Europos Sąjungos interesus, valstybės narės įgaliojamos ratifikuoti Protokolą, kuriuo iš dalies keičiama Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018PC0451&from=LT

[120]Europos Sąjunga, „Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“ žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016R0679&from=LT

[121] Europos Sąjunga „Europos Sąjungos pagrindinių teisių chartija“, *EUR-Lex,* 2016 m. spalio 17 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12016P/TXT&from=LT

asmens duomenų apsaugą. Šiame straipsnyje yra įvardijama, kokias pagrindines teises asmuo turi:

„16 straipsnis.

1. Kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą;

2. Europos Parlamentas ir Taryba, spręsdami pagal įprastą teisėkūros procedūrą, nustato fizinių asmenų apsaugos Sąjungos institucijoms, įstaigoms ir organams bei valstybėms narėms tvarkant asmens duomenis, kai vykdoma veikla yra susijusi su Sąjungos teisės taikymo sritimi, taisykles ir laisvo tokių duomenų judėjimo taisykles. Nepriklausomos įstaigos kontroliuoja, kaip laikomasi tų taisyklių."[122] Atkreiptinas dėmesys į Konvencijos Nr. 108 8 straipsnį, kuriame minima, kokią kiekvienas asmuo turi teisę į duomenų apsaugą.

Pagrindiniai šios Konvencijos įtvirtinti principai yra susiję su sąžiningu ir teisėtu asmenų duomenų tvarkymo procesu, kuriuo turėtų vadovautis teisėsaugos institucijos. Be kita ko, atkreiptinas dėmesys, kad Konvencija Nr. 108 buvo atnaujinta siekiant atitikti skaitmeninės eros iššūkius. Esminiai atnaujinimai yra susiję su toliau įvardintais klausimais, t. y. proporcingumu, duomenų minimizavimu, pareiga įrodyti atitikimą taikytiniems principams, ypatingai duomenų tvarkytojams ir vykdytojams, pareiga pranešti apie duomenų apsaugos pažeidimus, duomenų tvarkymo skaidrumu ir kitais papildomais saugikliais dėl duomenų apsaugos.[123]

Be jokios abejonės, galima teigti, kad šiuo metu didžiausias dėmesys yra kreipiamas būtent į Bendrąjį duomenų apsaugos reglamentą, kadangi šiuo reglamentu yra nustatoma asmens duomenų apsaugos teisinė sistema pasitelkiant netgi automatizuotas priemones. Pagal bendrojo duomenų apsaugos reglamento 4 straipsnį:

„Duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimais, ištrynimas arba sunaikinimas."[124]

Dar viena svarbi teisė, kurią reikia paminėti, yra teisė į privatų ir šeimos gyvenimą. Šiuo atveju vėlgi paminėtina ES pagrindinių teisių chartija, o būtent 7 straipsnis:

---

[122] Europos Sąjunga „Sutartis dėl Europos Sąjungos veikimo suvestinė redakcija" *Eur-Lex.*, žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A12012E%2FTXT

[123] „Modernisation of the Data Protection „Convention 108", *Council of Europe*, 2018 m. sausio 28 d., žiūrėta 2021 m. gruodžio 1 d., https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true

[124] Europos Sąjunga, „Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)" 2016 m. balandžio 27 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016R0679&from=LT

„*Kiekvienas asmuo turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas*.“[125] Taip pat yra akcentuojama, kad DI gali būti didelė grėsmė ar pavojus asmens privatumui.[126] Tai gali būti paaiškinama dviem aspektais, t. y. kad DI gali patekti į tradiciškai apsaugotą privačią erdvę bei dėl to, kad jis sugeba atrinkti ir perduoti asmeninius ir konfidencialius duomenis, galimai susijusius su asmens duomenimis.[127] Ši teisė yra itin glaudžiai susijusi su minėta teise į asmens duomenų apsaugą. Taip pat atkreiptinas dėmesys į 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje[128], šio ES priimto teisės akto, kuris yra įgyvendintas visose ES valstybėse narėse paskirtis yra užtikrinti saugumą elektroninėje erdvėje, o kilus saugumo pažeidimo grėsmei turi būti imtasi tinkamų ir skubių veiksmų, kad tokia grėsmė būtų pašalinta ir vartotojai apie saugumo pavojų būtų informuoti, dažniausiai tokia pareiga tenka duomenų valdytojui. Todėl galima daryti išvadą, kad privatumas, kaip ir teisė į duomenų apsaugą, yra viena iš jautriausių sričių, todėl itin didelis dėmesys turi būti skiriamas šių teisių apsaugojimui.

Nagrinėjant asmens apsaugos nuo DI ribas, yra paminėtinas ir žmogaus orumas, ES pagrindinių teisių chartijoje 1 straipsnyje yra įtvirtinta:

„*Žmogaus orumas yra neliečiamas. Jį reikia gerbti ir saugoti*.“ Šiuo atveju pabrėžiama, kad DI plėtojimas turi būti vykdomas taip, kad nebūtų pažeistas žmogaus orumas ir apsisprendimo teisė.[129] Žmogaus orumo apsauga, įskaitant apsisprendimo teisę ir autonomiškumą, yra viena iš svarbiausių teisių, kurią reikėtų ginti skaitmeninėje eroje. Todėl, reguliuojant DI sistemų veiklą, yra siūlytina akcentuoti ir užtikrinti žmogaus orumą ir jo apsaugą tokiu būdu, kad žmogaus gebėjimai ir intelektas nebūtų per daug ir pernelyg lyginami su DI sistemomis.

[125] Europos Sąjunga „Europos Sąjungos pagrindinių teisių chartija“, *EUR-Lex,* 2016 m. spalio 17 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12016P/TXT&from=LT
[126] Europos Parlamentas „Pranešimas su rekomendacijomis Komisijai dėl dirbtinio intelekto taikomų civilinės teisės nuostatų“, 2020 m. spalio 10 d., žiūrėta 2021 m. gruodžio 1 d., https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_LT.html
[127] *Ibid*
[128] Europos Parlamento ir Tarybos direktyva „dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), 2002 m. liepos 12 d., žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32002L0058&from=LT
[129] *Ibid*

3. EMPIRINIS TYRIMAS „Dirbtinio intelekto naudojimo teisėsaugos institucijų veikloje iššūkiai žmogaus teisių požiūriu“

Empirinio tyrimo metodologija

Sprendžiant klausimą, kokio tipo tyrimas tinkamiausias šiam darbui, buvo vertinamas kiekybinio ir kokybinio tyrimo metodų pagrįstumas, efektyvumas, būtinumas tyrimo uždaviniams pasiekti. Kiekybinis tyrimas pripažintas netinkamu, nes nagrinėjama tema yra pakankamai nauja ir reikalaujanti specifinių žinių. Nėra pakankamai statistinės informacijos tinkamam kiekybiniam tyrimui atlikti, be to, atliekant anketinę apklausą nebūtų pavykę rasti didelės imties tinkamų respondentų arba jų atsakymai būtų buvę neišsamūs ir nepagrįsti patirtimi. Pagrindinis skirtumas tarp kiekybinių ir kokybinių tyrimų — kiekybinio tyrimo atveju gaunami rezultatai dažniausiai išreiškiami skaičiais, procentais ir statistiniais ryšiais, o kokybinio tyrimo rezultatas yra tekstinio pobūdžio, nestruktūrizuotas, neturintis reprezentatyvumo, bet pateikiantis gilesnę ir platesnę informaciją, nei kiekybinių tyrimų.[130]

Tyrimo iškeltiems uždaviniams įgyvendinti buvo nuspręsta atlikti kokybinį tyrimą. Kokybinis tyrimas - tai toks tyrimas, kuris sociologijos, filosofijos, logikos ir individualaus stebėjimo priemonių pagalba padeda suprasti tam tikrą žmonių elgesį ir tokio elgesio priežastis.[131] Kokybinis tyrimas atskleidžia ne tik akivaizdžiai matomus dalykus, bet nagrinėja ir giliau esančius požiūrius, įsitikinimus ir vertybes.[132] Informaciją tyrimui nuspręsta rinkti atliekant ekspertinį pusiau struktūrizuotą interviu. Tokiam interviu parenkami ekspertai, kurie yra savo profesinės srities žinovai, turintys didžiausią kompetenciją analizuojamoje temoje ir galintys suteikti daugiausiai detalios informacijos apie tiriamą objektą, aptarti ir patikrinti tyrimo hipotezes, bei įvertinti įvairias tyrimo metodikas.

Pusiau struktūrizuotą ekspertinį interviu rekomenduojama naudoti tada, kai tyrėjas turi pasirengęs temų sąrašą, bet nori turėti laisvės interviu metu paklausti neparuoštų klausimų, kurie kyla bendraujant su pašnekovu. Taikydamas pusiau struktūrizuotą interviu tyrėjas gali lengviau suprasti tiriamą problemą ir atskleisti visiškai netikėtus ar nenumatytus problemos aspektus.[133] Šio tyrimo tikslinę grupę sudarė ekspertai ir pareigūnai, dirbantys ar kitaip susiję su DI

[130] Rimantas Tidikis, „Socialinių mokslų tyrimų metodologija“, *Lietuvos teisės universitetas*, (2003) 41-56, žiūrėta 2021 m. gruodžio 1 d., https://repository.mruni.eu/handle/007/15459?show=full
[131] *Ibid*
[132] Inga Gaižauskaitė ir Natalija Valavičinė „Socialinių tyrimų metodai. Kokybinis tyrimas“ Vilnius (2016) 35-38, žiūrėta 2021 m. gruodžio 5 d.
[133] Liudmila Rupšienė „Kokybinio tyrimo duomenų rinkimo metodologija“. Klaipėdos universitetas, 2007 m. sausio 8 d., 63-75, žiūrėta 2021 m. gruodžio 1 d., https://www.researchgate.net/publication/323497804_Kokybiniu_tyrimu_duomenu_rinkimo_metodologija

sistemomis bei technologijomis, atsižvelgiant į jų galimybes ir profesinį užimtumą, buvo pasirinktas pusiau struktūrizuoto interviu metodas.

Empirinio tyrimo tikslas ir uždaviniai

Tyrimo tikslas:

Išsiaiškinti, su kokiais iššūkiais žmogaus teisių požiūriu susiduriama taikant DI pagrįstas sistemas teisėsaugos institucijose.

Empirinio tyrimo imtis:

„Kokybiniame tyrime neverta siekti tikimybinės, atsitiktinai sudarytos imties, bet priešingai — reikia pasirinkti tokius atvejus, kurie informatyvūs tiriamuoju požiūriu. Kiekviename tyrime imties dydis ir konkretūs tyrimui pasirinkti imties vienetai iš esmės priklauso nuo tyrimo tikslų“.[134] Empiriniam tyrimui ekspertai buvo parinkti naudojant tikslinį grupių formavimą, remiantis jų patirtimi, kasdiene veikla ir darbo sritimi. Renkantis galimus kandidatus buvo analizuojamos teisėsaugos institucijų, kuriose naudojamos DI technologijos, funkcijos, taip pat buvo vertinama, kiek respondentas turi žinių tiriama tema, atsižvelgiama į jo darbines funkcijas. Visi respondentai su DI veikiančiomis sistemomis dirba tiesiogiai. Du respondentai buvo parinkti stebint socialinius tinklus, nes aktyviai dalinasi susijusiais straipsniais tiriama tema bei įvairiomis DI technologijų įžvalgomis. Taip pat vienas ekspertas buvo parinktas pagal kito eksperto rekomendaciją.

Sudarant ekspertų grupę tyrimui atlikti rekomenduojama įtraukti ne mažiau kaip 5 ekspertus. Prieš apklausiant ekspertus buvo paruošti du interviu planai (žr. Priedą Nr. 1 ir Priedą Nr. 2). Interviu planai buvo pateikti dviem skirtingoms asmenų grupėms: a) teisėsaugos institucijų darbuotojams, b) DI technologijų civiliams ekspertams. Pradedant interviu su abiem respondentų grupėmis buvo pristatytas magistro baigiamasis darbas, nurodyta rašomo darbo tema ir tyrimo tikslas, paminėta, kad vykdant interviu bus išlaikytas ekspertų anonimiškumas ir pateikiant rezultatus respondentams bus suteikti kodiniai pavadinimai. Antrosios respondentų grupės apklausos atvejutaip pat buvo pateikta visa pirminė informacija, tačiau šie interviu buvo orientuoti į DI sistemų technologus, civilius asmenis, kurie fiziškai prisiliečia prie DI sistemų

[134] Liudmila Rupšienė „Kokybinio tyrimo duomenų rinkimo metodologija“. *Klaipėdos universitetas*, 2007 m. sausio 8 d., 63-75, žiūrėta 2021 m. gruodžio 1 d., https://www.researchgate.net/publication/323497804_Kokybiniu_tyrimu_duomenu_rinkimo_metodologija

kūrimo, jų analizavimo bei įgyvendinimo, todėl kai kurie klausimai buvo labiau techninio pobūdžio.

Pirmąjį interviu klausimyną sudaro 8 klausimai, skirti teisėsaugos pareigūnams, kurie įvardyti kaip P1- P3.

Antrąjį interviu klausimyną sudaro 10 klausimų, skirti civiliais asmenims, kurie įvardyti kaip E1 - E2.

Empirinio tyrimo loginė eiga

Empirinis tyrimas buvo atliekamas 2021 lapkričio 10 – lapkričio 29 dienomis. Tyrimui buvo parinkti Valstybės sienos apsaugos, policijos, muitinės institucijų ekspertai (respondentai ekspertai) ir civiliai asmenys, kuriantys DI technologines sistemas (respondentai technologai). Tyrimui parinkti teoriniu, teisiniu ir praktiniu lygmeniu dirbantys specialistai. Atrenkant ekspertus buvo ieškoma specialistų, kurių darbo patirtis tiriamoje srityje yra ne mažesnė kaip 3 metai.

Su ekspertais buvo susiekta elektroniniu paštu arba per socialinį tinklą Facebook, informuojant juos apie norimą atlikti tyrimą. Respondentai buvo informuojami apie tai, kad jų vardai, pavardės, darbovietės nebus viešinamos ir bus išlaikytas anonimiškumas. Visi ekspertai, į kuriuos buvo kreiptasi, sutiko dalyvauti tyrime. Respondentams sutikus dalyvauti interviu, jiems buvo išsiunčiama papildoma informacija apie rašomą darbą, norimą sužinoti informaciją ir specialiai jiems orientuotas interviu klausimynas. Su trimis teisėsaugos pareigūnais buvo bendrauta tiesiogiai, paimta interviu (įrašas). Taip pat su vienu technologinės grupės ekspertu bendrauta tiesiogiai, (įrašytas interviu). Kitas technologinės grupės ekspertas pageidavo į interviu atsakyti el. paštu, pildant tekstinį dokumentą ir atsakant į pateiktus klausimus. Vienas technologinės grupės ekspertas pageidavo, kad interviu būtų vykdomas telefonu ir davė sutikimą dėl pokalbio įrašymo. Tais atvejais, kai su respondentu buvo bendraujama tiesiogiai imant interviu, pokalbio įrašas būdavo perklausomas ir jo stenograma perkeliama į tekstinio redaktoriaus dokumentą, pasinaudojant DI pagrindu veikiančia sistema pavadinimu „Lietuvių kalbos fonogramų automatinės transkripcijos tekstu paslauga“ ir „Lietuviško teksto analizė ir taisymas“, kurios priklauso Vytauto Didžiojo universiteto internetiniam puslapiui pavadinimu „Semantika“. Interviu trukmė - nuo 26 iki 55 minučių. Bendraujant telefonu ir darytų tiesioginių pokalbių įrašai taip pat buvo perklausomi ir jų stenogramos perkeliamos į tekstinio redaktoriaus dokumentą, pasinaudojant DI pagrindu veikiančia „Lietuvių kalbos fonogramų automatinės transkripcijos tekstu paslauga“ sistema. Pokalbio trukmė — 45 min.

Respondentų užpildytos anketos ir pokalbių stenogramos buvo kaupiamos ir, remiantis jomis, buvo atliekamas tyrimas. Šiame darbe pateikiama tik vieno respondento interviu atsakymas bei transkribuotų pokalbių tekstas,(netaisytas) (žr. Priedą Nr. 3) kuriame galima matyti vienos užpildytos anketos pavyzdį.

Kartu su tiriamaisiais klausimais nebuvo fiksuojama eksperto asmens informacija siekiant užtikrinti ekspertų konfidencialumą. Patogumo dėlei respondentams buvo suteikti kodiniai pavadinimai E1, E2, taip pat P1, P2, P3. Tyrimo rezultatuose būtent šiais kodiniais pavadinimais ir yra įvardijami ekspertai.

Empirinio tyrimo duomenų analizė

Pirmas klausimas, užduotas tiek teisėsaugos institucijų pareigūnams, tiek technologiniams ekspertams — *„Kaip, Jūsų nuomone, dirbtinis intelektas palengvino mūsų visų viešąjį ir privatų gyvenimą? Kokias svarbiausias problemas jis išsprendė? Kaip manote, kokios problemos bus išspręstos ateityje?“*

Respondentai P1 akcentuoja, kad DI iš dalies išsprendė tai, jog galima greitai ir dideliais kiekiais apdoroti pateiktą informaciją į tam konkrečiai suformuotus veiksmus, taip pat, kad DI iš dalies palengvino mūsų viešą gyvenimą. P2 teigimu, tai sukūrė laisvę rinktis, platesnį pasaulio pažinimą, kuris suteikia žmonėms daugiau galimybių ir pagundų, taip pat sukūrė didesnes grėsmes privačiam gyvenimui. Vis daugiau žmonių, nieko blogo nenutuokdami, kelia į socialinius tinklus informaciją apie savo asmeninį gyvenimą. Taip pat P2 akcentuoja, kad šiuo metu technologijos yra sustojusios kuriant naujas DI sistemas. Šiuo metu akcentuojami technologijų tobulinimo ir atnaujinimo procesai, kurių metu esamos programos modernizuojamos, įvedant naujas funkcijas ar algoritmus. Būtent dėl to šiuo metu plačiai analizuojama, kokios ir kaip esamos problemos gali būti išspręstos dėl technologijų pritaikymo, užtikrinant žmogaus privatų gyvenimą. P3 nuomone, DI sistemos palengvina darbą pareigūnams, kuo efektyviau ir greičiau atliekant paskirtas funkcijas. P3 tikisi, kad ateityje bus sumažintos netinkamai naudojamos informacijos apimtys.

Uždavus tą patį klausimą respondentams E1, E2, jie įvardijo, kad DI palengvino mūsų visų gyvenimą. E1 teigimu, DI sistemų pagalba įrašyta garso įrašą galima transkribuoti ir paversti tekstu ir kitomis sistemomis. Prieš 5-7 metus, apie tai buvo tik kalbama, tačiau šiandieniniu laikotarpiu yra plačiai taikoma. Pasak respondento E2, didžioji dalis visų veikiančių programų bei sistemų turi dalelę DI sistemos pradmenų, tai palengvina darbą, padidina darbo našumą įvairiose srityse. E1 nuomone, problemos dažniausiai iškyla ne dėl pačių DI pagrindu

veikiančių sistemų, bet dėl tų sistemų ir technologijų taikymo, kadangi jos gali būti taikomos skirtingais metodais ir būdais. E2 teigimu, DI pagrindu veikiančios sistemos užtikrina tolimesnę pažangą.

Apibendrinant pateiktą klausimą galima daryti išvadą, jog DI sistemos iš tiesų palengvina mūsų kasdienį gyvenimą, tačiau laikui bėgant atsiranda vis daugiau problemų jas taikant. Šios problemos kyla ne dėl galimų sistemos klaidų, bet dėl galimai netinkamai DI naudojimų technologijų. Problemų sprendimas visada išliks atviras klausimas, kadangi sistemos tobulėja ir vis dažniau pasitaiko sisteminių neatitikimų.

Antras klausimas ekspertams — *„Kaip manote, ar dirbtinio intelekto technologijos su Konstitucijoje numatytomis teisės normomis neprasilenkia? Pvz., teise į asmens privatų gyvenimą. Jei taip, tai kodėl?“*

Šiuo klausimu pasisakė E1, E2 kurie teigė, kad taikant DI technologijas priklauso nuo sukurto algoritmo ar tam tikros funkcijos, kuri atlieka numatytą veiksmą. E1 teigimu, technologija pati negali pažeisti įtvirtintų teisių, tačiau šių technologijų sistemos ir jų pritaikymas šiuolaikiniame pasaulyje gali sudaryti tam tikrus nuokrypius, kurie gali lemti teisės pažeidimus. Norint to išvengti, E1 papildo, kad privalu tinkamai reglamentuoti DI sistemų taikymą. Dėl to tam tikrais atvejais gali būti pažeidžiamos tam tikros teisės, tačiau tik išskirtiniais atvejais, pvz. tokia teisė į judėjimo laisvę, kai tiek keliuose, tiek miesto gatvėse yra sustatytos kameros, kurios fiksuoja asmens judėjimo kryptį, laiką. E2 teigia, kad kiekviena Konstitucijoje numatyta teisė šiais laikais gali būti labai lengvai pažeidžiama. DI sistemų pagrindu veikiančios technologijos tam tikrais atvejais pažeidžia teises, numatytas Konstitucijoje. Norint tokių pažeidimų išvengti, reikia įtvirtinti tinkamą technologijų taikymą, kuris numatytų, kaip turi būti naudojama ir kam ta gauta informacija gali būti pritaikoma.

Apibendrinant pateiktus ekspertų atsakymus, galima daryti prielaidą, kad DI technologijos gali tam tikrai atvejais prasilenkti su teisės aktuose numatytomis teisėmis į privatų gyvenimą, tačiau pasauliui plečiantis, tokių pažeidimų gali nepavykti išvengti. Būtent dėl to, pasak ekspertų, yra svarbus konkretus DI sistemų taikymo reglamentavimas. Šiuo reglamentavimu atsirastų galimybė užtikrinti, kad nebūtų pažeidžiamos teisės į privatų gyvenimą. Galbūt ateityje visose išsivysčiusiose šalyse atsiras kokybiški teisės normas įtvirtinantys teisės aktai, kurie neleis pažeisti teisės į asmens privatų gyvenimą.

Antras klausimas užduotas tiek pareigūnams, tiek technologijų ekspertams — „***Kalbant apie dirbtinį intelektą dažnai iškeliamas duomenų apsaugos ir privatumo klausimas. Tokios dirbtinio intelekto technologijos, kaip veido atpažinimo sistemos, yra laikomos į privatumą besibraunančia technologija. Kaip manote, ar galima rasti balansą tarp technologijų plėtros ir duomenų apsaugos?“***

Respondentai P1, P2, P3 vieningai atsakė, kad kiekvienu atveju balanso tarp technologijų plėtros ir duomenų apsaugos reikia ieškoti bandant pritaikyti technologijas reikiamai krypčiai. P1 teigimu, šie balansai nėra atrandami, kadangi nedaugelis diskutuoja apie tai ir turbūt net nesusimąsto, kad gali iškilti tokie klausimai. Tačiau, pasak P1, kiekvienu atveju, asmuo yra pats atsakingas už savo veiksmus ir duomenų apsaugą. Atsižvelgiant į tai, apie duomenų apsaugą kalbėti vis sunkiau, kai šiuolaikiniai žmonės vis dažniau internetiniuose tinkluose viešai pateikia savo asmeninius duomenis, nurodo tam tikrus pomėgius ar net savo gimimo datas ir kitą asmeninę informacija. Dėl to, P2 teigimu, žmonės privalo būti patys atsakingi už savo duomenų apsaugą. P2 nuomone, duomenų apsauga labai stipriai priklauso ir nuo sistemos kūrėjo patikimumo, kiek kūrėjas yra įdėjęs pastangų, kad jo sistemoje esantys asmens duomenys nebūtų nukreipti netinkama linkme ir nebūtų paviešinti. Pasak P3, reikia tobulinti šių DI technologijų tinkamą taikymą. Technologijos visada bus žingsniu priekyje ir ne visada užtikrins tinkamą duomenų apsaugą.

Šis klausimas taip pat buvo užduotas ir technologijų ekspertams. E1, panašiai kaip ir anksčiau kalbinti respondentai, teigė, kad visada reikia atrasti technologijų balansą. Sistemos, patekusios į netinkamas rankas, gali padaryti daug žalos duomenų apsaugai, pažeisti žmogaus teises. E2 nuomone, netinkamai atrastas balansas gali padaryti didelę žalą duomenų apsaugai. Netinkami gauti veido atpažinimo sistemų duomenys ar biometriniai duomenys, gali sudaryti papildomų problemų, į kurias privalu atkreipti dėmesį taikant DI technologijas.

Atsižvelgiant į tai, kas išdėstyta, galima daryti išvadą, kad P1, P2, P3, E1 ir E2 supranta, kad kiekvienu atveju fizinis asmuo yra atsakingas už savo duomenų apsaugą, kadangi niekas kitas be paties asmens asmeninės informacijos neturi arba negali gauti prieigos prie tokių duomenų, tik išskirtiniais atvejais asmenys, turintys reikiamus leidimus, turi teisę ir galimybę kaupti asmens duomenis. Vis dažniau atsiranda įvairių straipsnių, kad naudojant įvairiausias DI pagrindu veikiančias sistemas yra pažeidžiama duomenų apsauga. Duomenų apsauga ir technologijų plėtra, pasak pareigūnų, turėtų judėti viena šalia kitos, tačiau šiuo metu duomenų apsauga prasilenkia su tinkamu sistemų naudojimu.

Trečias klausimas ekspertams — *„Kaip manote, ar gauti duomenys pasitelkiant dirbtinio intelekto sistemas, yra neviešo pobūdžio? Kokia gali būti sistemos kūrėjo atsakomybė už gautų duomenų išviešinimą?“*

Šiuo klausimu E1 ir E2 pateikė skirtingus pastebėjimus į pateiktą klausimą. E1 pasisakė, kad priklausomai nuo to, kokioje vietoje ir kaip šie duomenys gauti, priklauso jų apsaugos lygis, kadangi daugelyje DI pagrindu veikiančių sistemų pateikiami duomenys yra saugomi ir bet kas negali turėti prieigos prie duomenų bazių. Tačiau labai dažnai atsiranda tretieji asmenys, veikiantys tarp asmens ir DI pagrindu veikiančios sistemos, kurie esančius sistemose duomenis nutekina arba paviešina. E1 teigimu, tai priklauso nuo sistemos kūrėjo, kuris atlikdamas tam tikras funkcijas privalo užtikrinti, kad asmens pateikti duomenys būtų saugūs. Pasak E2, DI sistemų kūrėjai turi užtikrinti, kad sukaupta nenaudinga informacija būtų panaikinama, kad tretieji asmenys negautų prieigos prie informacijos. Anot E1, taikant atsakomybę turėtų būti atsižvelgiama į tai, ar sistemos kūrėjas užtikrino, kad asmens duomenys nebūti pažeisti. E1 pateikia puikų pavyzdys apie visai nesenai Lietuvoje nuskambėjusį atvejį apie asmens duomenų nutekinimą „CityBee“. Tai nulėmė, jog įmonės sistemų kūrėjai neužtikrino reikiamos sistemos apsaugos, todėl atsirado „plyšys“ tretiesiems asmenims tuo pasinaudoti. E2 manymu, atsakomybė turi būti skirta tam, kas yra atsakingas už tinkamą sistemų veikimą.

Remiantis pateiktomis nuomonėmis galima išvada, kad kiekvienu atveju privalu atsižvelgti į reikiamą pateiktų asmens duomenų apsaugą, kuri turėtų būti užtikrinama kūrėjų, todėl atsakomybė gali būti vertinama įvairiai. Taip pat situacija vertintina pagal tai, kaip pats asmuo pateikė savo duomenis, ar nebuvo padaryti pažeidimai, ar prieš pateikiant savo duomenis ar asmuo buvo įspėtas, jog duomenys gali būti panaudoti visai kitiems tikslams. Todėl įvairiuose internetuose puslapiuose, suvedus savo asmens duomenis, dažniausiai paskutinėje eilutėje būna nuorodą, kuria reikia patvirtinti, kad asmuo susipažino su puslapio valdytojo sąlygomis ir sutinka, kad asmens duomenys būtu pateikti puslapio kūrėjui. Atsižvelgiant į praktinę pusę, žmonės neperskaitę minėtų taisyklių įvairiuose pateikia duomenis, kurie nėra tinkamai saugūs ir neužtikrina, kad pateiktais duomenimis niekas kitas negalės pasinaudoti. Todėl asmenims privalu atkreipti dėmesį, norint užtikrinti duomenų saugumą.

Trečias klausimas pareigūnams — *„Ar dirbtinio intelekto sistema teikia naudos visuomenės saugumui? Ar taikomi metodai yra pranašesni už kitus tradicinius teisėsaugos institucijų metodus?“*

Respondentai P1, P2, P3, turėjo panašią nuomonę, jog tinkamas sistemų DI taikymas yra svarbus užtikrinant visuomenės saugumą. DI sistemų taikymas teisėsaugos institucijose suteikia papildomų funkcijų, kuriomis naudojantis iš dalies gali būti užtikrintas visuomenės saugumas. P1 pažymi, kad tinkamai naudojamos informacinės ir DI sistemos užtikrina visuomenės saugumą. Visi respondentai sutinka, kad šiuolaikiniai sistemų taikymai yra pranašesni už tradicinius metodus. Pasak P2, kuo toliau, tuo labiau DI sistemos bus pranašesnės už tradicinius teisėsaugos institucijų metodus. Respondentai P1, P2, P3, turėjo panašia nuomone, jog tinkamas sistemų DI taikymas yra svarbus užtikrinant visuomenės saugumą. DI sistemų taikymas teisėsaugos institucijose suteikia papildomų funkcijų, kuriomis naudojantis iš dalies gali būti užtikrintas visuomenės saugumas. P1 pažymi, kad tinkamai naudojamos informacinės ir DI sistemos užtikrina visuomenės saugumą. Visi respondentai sutinka, kad šiuolaikiniai sistemų taikymai yra pranašesni už tradicinius metodus. Pasak P2, kuo toliau, tuo labiau DI sistemos bus pranašesnės už tradicinius teisėsaugos institucijų metodus. P3 nuomone, DI sistemų pagalba darbas tampa efektyvesnis, o DI taikomi metodai tampa puikiu įrankiu darbo spartinimui. Respondentai teigia, kad DI sistemų pagalba jiems palengvina darbą, suvedus tam tikrus duomenis sistemos atpažįsta ir pateikia tokiu, kokių buvo užklaustą. Taip pat teigė, kad DI sistemų pagalba, atliekant darbus priimami greitesni sprendimai, negu būtų taikoma primityviais būdais.

Iš pateiktų atsakymų vienareikšmiškai galima susidaryti nuomonę, kad teisėsaugos institucijos nauji technologiniai metodai yra pranašesni už senuosius visuomenės saugumą užtikrinančius metodus. Remiantis tuo, teisėsaugos institucijose privalu diegti vis naujas sistemas, kurios leistų efektyviau užtikrinti visuomenės saugumą. DI technologijų taikymas teisėsaugos institucijose kiekvienais metais vis tobulėja ir sparčiais žingsniais juda pirmyn. Deja, Lietuvos teisėsaugos institucijose, tik labai nedidelė dalis finansavimo yra skiriama technologijų plėtrai.

Ketvirtas klausimas pareigūnams — *„Kaip, Jūsų manymu, pareigūnai gali pritaikyti dirbtinio intelekto pagrindu gautus sistemos rezultatus, pvz., modeliuojant būsimas grėsmes, kuriant rizikos profilius, nustatant tam tikrus algoritmus?“*

P1 teigia, kad norint jog DI sistemos tinkamai veiktų, visų pirma, DI pagrindu veikiančiai sistemai reikia pateikti turimus ankstesnius pavydžius, kuriais remiantis sistema galėtų atpažinti neatitikimus. Šie būdai jau dabar palengvina pareigūnams darbą, P1 tikisi, kad sistema ateityje bus dar labiau patobulinta. Šiuos neatitikimus suprogramuotos DI pagrindu sistemos gali greitai atpažinti ir pateikti išvadą. P2 teigimu, DI sistemos palengvina darbą, nes jos gali apdoroti didelius informacijos kiekius, kurių fiziniam asmeniui reiktų begalės laiko. P3 nuomone, fiksuojant tam tikrus įvykius galima sudaryti statistinius duomenis, nukreipti darbo našumą ten, kur labiausiai reikia.

Remiantis tuo, kas išdėstyta, galima teigti, kad kiekviena DI pagrindu sistema, kuri pareigūnų naudojama teisėsaugos institucijose, pagerina darbo kokybę ir informacijos apdorojimo tikslumą. DI sistemos nepervargsta, neatlieka netinkamų veiksmų. Derėtų atkreipti dėmesį į tai, jog dažnai pasitaiko neatitikimų ar klaidų, kurios atsiranda dėl to, kad nebuvo tinkamai išanalizuotos. Kaip pavyzdį galima įvardinti, jog, nuskaitant valstybinius numerius ar kitus identifikavimo kodus, gali atsirasti sutapimų ar neatitikimų, dėl kurių gali būti suformuota klaidinga nuoroda ar klaidingas atpažinimas. Šia klaida vadovaujantis gali būti priimamas netinkamas sprendimas. Iš mano darbinės aplinkos pavyzdys, sistemoje suformuotas algoritmas, kad gavęs tam tikrą nuorodą suformuotų ir atsiųstų pranešimą. Tačiau sistema, atpažinusi tik dalį reikiamo identifikavimo, siunčia man užklausą su klaidinga informacija, nors DI sistema atpažino sutapimą, tačiau ten yra klaida. Šias klaidas DI sistemos atpažįsta ir gali užtikrinti, jog tinkamai suformavus užduotis bei nuolatos tobulinant turimas ir būsimas DI pagrindu sistemas galėtų būti sumažinama DI sistemų klaidų rizika.

Ketvirtas klausimas ekspertams — *„Ar Jūsų manymu institucijos, leidžiančios sistemų kūrėjams gauti prieigą prie informacijos, užtikrins, kad informacija būtų naudojama pagal paskirtį? Ar yra galimybė vykdyti atvirą šios informacijos stebėjimą ar kontrolę?“*

E1 ir E2 teigimu, DI pagrindu veikiančios sistemos neužtikrins tinkamos prieigos DI kūrėjams prie duomenų. E1 nuomone, DI sistemoms reikia konkrečios apsaugos, kurią turi užtikrinti kūrėjai. E1 teigimu, geriausia būtų turėti konkrečias teisės aktų lygmenyje įtvirtintas sankcijas, galbūt baudas, kurios užtikrintų atitinkamą atsakomybę už šių sistemų pažeidimą. Taip pat, E2 teigimu, institucijos, kurios naudoja DI pagrindu sistemas, privalo suteikti tam tikrus

reikalavimus sistemų kūrėjams, kurie užtikrintų pilniausią sistemų apsaugą. Taip pat, E2 teigimu, nėra tokių galimybių, kad būtų užtikrinamas sklandus informacinių duomenų saugojimas, dėl to, kad žmonės, kuriems suteiktos prieigos prie informacijos, gali būti korumpuoti ar turėti kitų tikslų.

Darytina išvada, jog kiekviena institucija turi skirtingų informacinių duomenų ir DI pagrindu veikiančių sistemų. Šias dažniausiai administruoja asmenys, neturintys kompetentingų žinių, susijusių su konkrečia institucija. Taip pat kiekviena, taip pat ir valstybinė, institucija privalo imtis visų priemonių tam, kad užtikrintų, jog kūrėjai, turėdami prieigą prie informacijos, jos nepaviešintų ar kitaip nepažeistų. Su tokiomis sistemomis turėtų dirbti tik tinkami paruošti ir patikrinti asmenys, kad būtų užtikrintas sistemose esamų duomenų saugumas.

Penktas klausimas pareigūnams — *„Kaip manote, ar pakanka teisės aktų, kurie reglamentuoja teisėtą ir efektyvų dirbtinio intelekto technologijų taikymą teisėsaugos institucijose?“*

P1 teigimu, yra labai sudėtinga vertinti ši klausimą, tačiau galima susidaryti išvadą, kad nepakanka. Taip pat ekspertas teigia, kad yra bandoma surasti tinkamą balansą, kuris užtikrintų teisės aktų taikymą. Taip pat P1 priduria, kad pilnaverčiam DI taikymui svarbu gauti klaidingos informacijos, kad ši padėtų tobulinti DI sistemas. Būtent dėl to šiuo metu pasaulyje diskutuojama, kokie DI veiksmai yra teisėti, kokie ne, ką pažeidžia, ko nepažeidžia. Tačiau P1 ir P2 teigimu, sudėtinga pritaikyti teisės aktus, kadangi niekas nežino, kaip šios technologijos vystysis toliau. P2 teigimu, dažniausiai teisės aktai yra nagrinėjami po kažkokių įvykių ar sistemų atsiradimų, kurie galbūt pažeidžia tam tikras teisės aktuose numatytas normas. P3 teigimu, šiuo metu yra tik iš dalies apibrėžtas teisinis reguliavimas. P3 nuomone reikalingas toks, kuris užtikrintų tinkamą ir nepažeidžiamą teisės aktų funkcijų atlikimą, tokių kaip laisvas asmenų judėjimas ar neteisėtas duomenų rinkimas.

Gali susidaryti išvadą, kad teisės aktai šiek tiek atsilieka nuo DI technologijų plėtros. Būtent todėl pasaulyje plačiai analizuojama tolimesnė DI technologijų ateitis. Šiomis technologijos tobulėjant, teisės aktai privalės būti pritaikyti prie esamos situacijos, priešingu atveju gali kilti žmonių pasipriešinimai, kai technologijos peržengs teisės aktuose numatytas ribas. Europoje yra analizuojami, teisės aktai kuriais bus numatytas tinkamas sistemų taikymas.

Šeštas klausimas pareigūnams — *„Kokias žinote dirbtinio intelekto pagrindu veikiančias sistemas teisėsaugos institucijose? Kokios, Jūsų manymu, labiausiai pasiteisinusios dirbtinio intelekto pagrindu veikiančios technologijų sistemos teisėsaugos*

institucijose? Pvz. „HERTA“ - veido atpažinimo sistema, „D4FLY“ - tapatybės ir dokumentų klastojimo nustatymas keliaujant, „PoliScan FM1“ - greičio matavimo prietaisai (trikojai), „Bloomberg“ - veido atpažinimo sistema.“

P1, P2 teigė, jog minėtos sistemos yra girdėtos ir tinkamai veikia praktikoje. P1 teigimu, šių technologinių sistemų yra daugybė ir įvairiausių. Minėtos programos yra daugiau naudojamos užtikrinant viešąją tvarką. P1 nuomone, teisėsaugos institucijos Lietuvoje neišgali skirti didelio finansavimo tam, kad įsigytų pasaulyje jau dabar plačiai naudojamas sistemas. Tai pat, P1 teigimu, teisinėje valstybėje užtrunka laiko, kol atsiranda galimybės įsigyti modernesnes technologijas. P2 teigimu, technologijos sparčiai modernėja ir valstybė, įsigijusi sistemas, privalo jas atnaujinti arba taikyti jau kitas sistemas, kurios atlieka dar efektyvesnes funkcijas. Jau keletą metų P1 ir P2 darbinėje aplinkoje yra analizuojamos kitose valstybėse taikomos DI pagrindu veikiančios sistemos, kurios užtikrina tinkamą institucijos funkcijų atlikimą. Abu respondentai sutinka, kad labiausiai pasiteisinusios yra veido atpažinimo sistemos, kurios, pasak pareigūnų, gali žymiai geriau atpažinti įvestus algoritmų sutapimus ar neatitikimus. P2 teigimu, viena iš naujausių technologijų yra tam tikrų akiai atrodančių panašių daiktų atpažinimas ir palyginimas, pvz., transporto priemonių iš nuotraukos nustatymas (ar tai yra ta transporto priemonė, kuriai priklauso valstybiniai numeriai, ar tai yra kita transporto priemonė). Ši sistema, pasak P2, yra dar tik bandoma, bet tikimasi, kad suteiks papildomos pagalbos pareigūnams. O respondento P3 nuomonė buvo kitokia. Anot jo, pilnai veikiančių DI sistemų teisėsaugos institucijose nėra, yra tik suvestiniai algoritmai, kurie atlieka tam tikras numatytas sistemines funkcijas.

Taigi, darytina išvada, kad teisėsaugos institucijose yra plačiai taikomos DI pagrindu veikiančios sistemos, tačiau dėl nedidelio finansavimo šių technologijų plėtra užtrunka ilgą laiką, todėl pagaliau įsigijus sistemas, tuo metu jau būna atsiradusios naujos dar efektyvesnės sistemos. Valstybė tik iš dalies suteikia tinkamą plėtrą ir finansavimą naujų sistemų įsigijimui ir taikymui.

Šeštas klausimas ekspertams — *„Ar dirbtinio intelekto sistema teikia naudos visuomenės saugumui? Ar taikomi metodai yra pranašesni už kitus tradicinius teisėsaugos institucijų metodus?“*

E1 ir E2 teigimu, DI sistemos vienareikšmiškai teikia naudą teisėsaugos institucijoms. E1 manymu, be DI taikomų metodų būtų sudėtinga išaiškinti įvairiausius nusikaltimus. E2 nuomone, didžioji dalis nusikaltimų persikelia į virtualią erdvę, dėl to DI pagrindu veikiančios sistemos, tinkamai suprogramuotos gali atpažinti ir nustatyti virtualius nusikaltimus. E1 teigia,

kad DI metodai yra pranašesni už tradicinius dėl to, kad tinkamai suformuota užduotis gali atpažinti neatitikimus, kurių fiziškai nebūtų galima atpažinti. Taip pat DI pagrindu veikiantys metodai yra labai naudingi kovojant su kibernetiniais nusikaltimais.

Atsižvelgiant į ekspertų įžvalgas galima teigti, kad teisėsaugos institucijoms DI pagrindu veikiančios sistemos yra naudingos. Jos suteikia tam tikros specifinės saugos, kurią fiziškai būtų sudėtinga užtikrinti. DI pagrindu veikiančios sistemos padeda užtikrinti tam tikrą funkcijų atlikimą. Tradiciniais metodais pasaulyje tampa vis sudėtingiau užtikrinti visuomenės saugumą, išaiškinti nusikaltimus, užkirsti jiems kelią, nes žmonės ir technologijos vis pažangesnės ir spartesnės.

Septintas klausimas pareigūnams, aštuntas klausimas ekspertams — *„Kas, Jūsų nuomone, nutiks, kai teisėsaugos institucijose naudojama dirbtinio intelekto sistema padarys klaidą?“*

P1 teigimu, DI sistema neuždeda antrankių ir nepriima galutinių sprendimų. DI gali padaryti klaidą, tačiau galutinį sprendimą, įvertinęs situaciją, priims fizinis asmuo. Pasak P2, šis klausimas dabar yra analizuojamas visame pasaulyje, kadangi sudėtinga yra įrodyti veiksmus, kuriuos atliko sistema. Puikus pavyzdys, kai DI sistemų pagrindu veikianti kamera užfiksavo pažeidimą, kuomet asmuo, vykdamas automobiliu iš stomatologo, laikė ranką prie veido šono. DI pagrindu veikianti sistema užfiksavo, kad asmuo laikydamas ranką prie veido kalba telefonu. Sistema, pamačiusi šį vairuotojo veiksmą, užfiksavo ir automatiškai sugeneravo pažeidimo protokolą transporto priemonės savininkui. Žinoma, šią bylą laimėjo fizinis asmuo, kuris įrodė, kad sistema klaidingai sugeneravo protokolą. P2 nuomone, reikia tobulinti DI sistemas. P3 pažymi, kad šiuo metu teisėsaugos institucijose nėra pilnos sistemos, kuri veiktų pasitelkdama tik DI veiksmus. P3 nuomone, privalu kiekvieną DI pastebėtą ar užfiksuotą neatitikimą patikrinti fiziniam asmeniui.

Iš pateiktų atsakymų galima daryti išvadą, kad negalima leisti sistemai priimti galutinių sprendimų. Taip pat darytina išvada, kad kiekvienu atveju DI konstatuotus pažeidimus ar neatitikimus būtina fiziškai patikrinti ir įvertinti riziką prieš priimant galutinį sprendimą.

Septintas klausimas ekspertams — *„Kokios Jums žinomos dirbtinio intelekto technologijos yra labiausiai pasiteisinusios? (Teisėsaugos institucijose, medicinos srityje, transporto logistikoje).“*

E1 nuomone, Lietuvoje viena iš labai plačiai taikomų naujovių — elektroninis parašas, kuris kitose valstybėse nėra plačiai naudojamas. Medicinoje technologijos taip pat yra žengusios didelį žingsnį atpažįstant galimas ligas iš vaizdo analizių. E2 įvardija, kad technologijos yra išplėtotos tiek medicinoje, tiek transporto srityje, tačiau teisėsaugos institucijos visada eina paskui privatų sektorių, kadangi privatus sektorius turi didesnes galimybes savo veikloje pritaikyti technologijas, tai padaroma ženkliai paprasčiau nei teisėsaugos institucijose. E1 teigimu, teisėsaugos institucijoms trūksta lėšų, kad galėtų efektyviai taikyti sukurtas DI technologijas.

Išanalizavus ekspertų nuomonę, galima daryti išvadą, kad teisėsaugos institucijoms yra skiriamas mažas finansavimas naujų DI technologijų taikymui. Didelės įmonės, turinčios papildomų lėšų, gali taikyti pažangiausias DI technologijas. Taip pat galima pabrėžti, kad Lietuvoje yra nemažai specialistų, kurie kuria, taiko naujas DI pagrindu veikiančias sistemas įvairiose institucijose. Didžioji dalis specialistų labiau linkę DI technologijas taikyti privačiame sektoriuje.

Aštuntas klausimas pareigūnams — *„Kaip manote, kokios dirbtinio intelekto inovacijos yra perspektyviausios kalbant apie visuomenės saugumo užtikrinimą?“*

P1 ir P2 teigimu, atsakyti į ši klausimą ir išskirti pačias perspektyviausias yra neįmanoma. Kiekvieną dieną pasaulyje atsiranda vis naujų DI sistemų. P1 nuomone, kiekviena DI technologija yra savaip perspektyvi, duodanti tam tikrą naudą visuomenei, tačiau apie visuomenės saugumo užtikrinimą sudėtinga kalbėti, kadangi technologijų inovacijos, iš vienos pusės, gali užtikrinti saugumą, iš kitos jį pažeisti. P2 nuomone, sistemų kūrėjai gali DI pagrindu sistemas pritaikyti įvairiausiomis kryptimis. P2 nuomone, didžiąją dalį visuomenės saugumo užtikrina teisėsaugos institucijos, kurioms būtinai reikia naujų technologinių sprendimų, kad galėtų užkirsti kelią būsimiems nusikaltimams. P3 teigimu, visuomenė privalo pati užtikrinti savo saugumą, technologijos saugumą gali užtikrinti tik iš dalies.

Šio klausimo atsakymo pagrindu galima formuluoti išvadą, kad teisėsaugos institucijose naudodamos DI technologijos, kurios iš dalies užtikrina visuomenės saugumą, informacijos srautus ir kitus šaltinius, kuriuose yra kaupiama skirtingo pobūdžio informacija.

Devintas klausimas ekspertams — *„Kaip manote, į kurią dirbtinio intelekto technologijų pusę turėtų būti nukreipti tyrimai ir inovacijos? Kokie tyrimai ar inovacijos Jums įdomiausios?“*

E1 teigimu, įdomiausia DI technologija yra biometrinių duomenų nuskaitymas ir pritaikymas DI sistemose. E1 teigimu, biometriniai duomenys užtikrintų aukščiausią apsaugą, kadangi identiškai tapačių duomenų nėra. Tai, pasak E1, bus taikoma netolimoje ateityje dar plačiau nei yra taikoma šiuo metu. Anot E2 teigimu, tyrimai turėtų būti dar labiau nukreipti į medicinos sritį, kurios pagalba būtų galima užtikrinti žmonių sveiką gyvenimą.

Iš pateiktų atsakymų galima daryti išvadą, kad ekspertai yra linkę į skirtingas tyrimų sritis. Tai yra natūralu, kadangi technologijų sritis yra labai plati, todėl apibrėžti, kur efektyviausia būtų taikyti DI tyrimus ir inovacijas, yra sudėtinga.

Dešimtas klausimas ekspertams — *„Kaip vertinate lietuvių pasiekimus dirbtinio intelekto srityse?“*

Lietuvių pasekimai yra labai perspektyvūs lyginant su kitos Europos valstybėmis. E1 nuomone, Lietuvoje yra labai daug įmonių, kurios savo veikloje taiko DI pagrindu veikiančias sistemas. Viena populiariausių sistemų yra „Vinted“, kuri įsitvirtino rinkoje pasauliniu mastu. Taip pat yra įvairiausių kompanijų, kurios savo darbo specifiką patiki robotizuotai technikai, kuri iš dalies veikia DI sistemų pagrindu. Taip pat medicinoje Lietuva neatsilieka taikydama DI sistemas. E2 turi informacijos, kad Lietuvoje yra kuriama sistema, kuri išskiria COVID-19 baltymus ir leidžia toliau juos tirti. E2 nuomone, Lietuva yra pažengusi DI taikyme, tačiau reikalingas dar didesnis finansavimas DI technologijų ir sistemų kūrimui. Taip pat Lietuva logistikos srityje yra pažengusi ir taiko įvairias sistemas, tokias kaip „Clipperon“, kuri leidžia užtikrinti saugų ir efektyvų krovinių pristatymą.

Apžvelgiant į gautus atsakymus, susidaro nuomonė, kad Lietuvoje yra didelių pasikeitimų DI technologijų ir sistemų veikloje. Pasak respondentų, Lietuvai, norint dar labiau būti perspektyvesnei, reikia skirti finansavimą, kuris užtikrintų DI taikomų priemonių kaitą.

IŠVADOS

1. Pastaruoju metu dažnas diskusijų ir tyrinėjimų objektas yra DI technologijos ir jo pagrindu veikiančios sistemos, kurios įvairiai vertinamos teisininkų, mokslininkų ir praktikų. Vieni autoriai, apibrėždami DI sąvoką, labiau pabrėžia informacinių technologijų savarankiškumą priimant protingus sprendimus, kiti labiau akcentuoja žmogaus įtaką DI sistemoms joms analizuojant ir atrandant reikalingą informaciją iš turimo duomenų rinkinio priimant atitinkamą sprendimą. Darytina išvada, kad DI sąvoka kol kas nėra tiksli, norint tinkamai ją apibrėžti reiktų analizuoti jo veikimo principus. Šiuo metu Europos Sąjungos mastu yra bandoma įtvirtinti DI sąvoką bei apibrėžti veikimo principus.

2. Teisėsaugos institucijose dažnai susiduriama su DI sistemomis, jų pagalba yra užtikrinama viešoji tvarka bei išaiškinami įvairūs nusikaltimai, analizuojamos galimos grėsmės. Taikant teisėsaugos institucijose DI pagrindu veikiančias sistemas gali kilti nesklandumų dėl šių sistemų taikymo - gali būti pažeidžiamos, suvaržomos žmogaus teisės. Su šia problema susiduria visos pasaulio valstybės, tačiau vienos valstybės turi įtvirtinusios konkretesnes DI technologijų ir jų sistemų teisėtumą užtikrinančias teisės normas, kitos pakankamo teisinio reguliavimo neturi. Taikant DI veiklą reguliuojančius teisės aktus, teisėsaugos institucijos privalo atsižvelgti į šių sistemų teisingą ir teisėtą naudojimą. Kiekviena tiek užsienio, tiek Lietuvos teisėsaugos institucija DI pagrindu veikiančias sistemas taiko skirtingai, naudodama skirtingus teisinius instrumentus. Magistro baigiamojo darbo metu buvo analizuotos teisėsaugos institucijose taikomos DI pagrindu veikiančios sistemos ir jų veiklos principai, galimos grėsmės, taip pat galimi žmogaus teisių pažeidimai taikant šias sistemas.

3. Analizuojant kokybinio tyrimo medžiagą akivaizdu, jog respondentai atskleidė aktualios ir reikšmingos informacijos apie DI technologijų ir sistemų taikymo apimtį teisėsaugos institucijose. Jie visi sutiko su nuomone, kad nereglamentuotai ir netinkamai taikomos DI technologijos gali pažeisti žmogaus teises. Respondentai pabrėžė, kad darbo metu dažnai susiduria su taikomų DI technologijų ir sistemų teisiniu reguliavimu, su tinkamų specialistų trūkumu bei kompetencijų stoka norint pilnai išnaudoti turimas ir būsimas sistemas. Kaip vieną iš svarbiausių dalykų respondentai pažymėjo, kad trūksta reguliaraus bei užtikrinančio naujų DI pagrindu veikiančių technologijų finansavimą. Tačiau, pasak respondentų, yra vilties, kad kylant ekonomikai technologijų finansavimas padidės. Jų teigimu, šiuo metu kiekviena teisėsaugos institucija be DI pagrindu veikiančių sistemų neužtikrintų pilnų teisėsaugos institucijai priskirtų uždavinių įgyvendinimo.

4. Nagrinėjant teisėsaugos institucijų asmens duomenų apsaugos DI ribas, darbe minimos žmogaus teisės ir laisvės, kurios yra numatytos ES pagrindinių teisių chartijoje, ir iš

kurių atsiranda ES valstybėms narėms bendrų konstitucinių tradicijų ir tarptautinių įsipareigojimų užtikrinti tinkamą teisių vykdymą. Šiuo atveju pabrėžiama, kad DI sistemos ir technologijų plėtojimas turi būti vykdomas taip, kad nebūtų pažeistos žmogaus teisės ir laisvės. Žmogaus teisų apsauga, įskaitant ir apsisprendimo teisę ir autonomiškumą, yra vienos iš svarbiausių teisių, kurias reikėtų ginti skaitmeninėje eroje. Todėl, reguliuojant DI sistemų veiklą, yra siūlytina užtikrinti žmogaus orumą ir jo duomenų apsaugą.

PASIŪLYMAI:

1. Iki šio nėra numatyta teisėsaugos institucijų atsakomybė už netinkamai naudojamus DI sistemų duomenis. Todėl siūlau papildyti „Lietuvos Respublikos policijos veiklos įstatymą“ Nr. VIII-2048, I skyriuje numatytame 9 straipsnyje, kad DI sistemų duomenys būtų tvarkomi teisės aktuose numatytais veiksmais.

2. Siūlau Lietuvos Respublikos teisėsaugos institucijoms lokaliniais, instituciniais teisės aktais apibrėžti konkrečias DI taikomas technologijas ir sistemas, taip pat atsižvelgiant į kitų valstybių gerąją praktiką taikant DI sistemas skirti papildomą kasmetinį finansavimą DI plėtrai Lietuvos teisėsaugos institucijose, kadangi atlikus teisėsaugos pareigūnų nustatyta, kad pareigūnai susiduria su DI pagrindu veikiančių sistemų bei technologijų veiklos neefektyvumu. Šis DI pagrindu platesnis veikiančių sistemų integravimas užtikrintų sklandesnį teisėsaugos institucijų darbą ir pagerintu darbo rezultatus.

LITERATŪRA:

Teisės aktai:

1. „Lietuvos Respublikos Konstitucija“. Valstybės Žinios, 1992, Nr. 33-1014. Žiūrėta 2021 m. gruodžio 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.1890/asr
2. Europos Komisija „Europos Komisijos Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais sukurtoje DI apibrėžtyje“ 2018 m. gruodžio 7 d.795 galutinis. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0011.02/DOC_2&format=PDF
3. „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“ LRS *Valstybės žinios*, 1995-05-16, Nr. 40-987. Žiūrėta 2021 m. gruodžio 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841
4. Europos Komisija „Baltoji Knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ 2020 m. vasario 19 d. 65 galutinis. Žiūrėta 2021 m. gruodžio 1 d. https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf
5. Europos Komisija „Europos Parlamento ir Tarybos reglamentas, kuriuo dėl Europolo bendradarbiavimo su privačiais subjektais, Europolo atliekamo asmens duomenų tvarkymo padedant atlikti nusikalstamų veikų tyrimus ir Europolo vaidmens mokslinių tyrimų ir inovacijų srityje iš dalies keičiamas Reglamentas“ *EUR-Lex*, 2020 m. gruodžio 9 d. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52020PC0796&from=LT
6. Europos Komisija „Komisijos komunikatas dėl ES saugumo sąjungos strategijos“. *EUR-Lex*, 2020 m. liepos 24 d. 605 galutinis. Žiūrėta gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:52020DC0605
7. Europos Komisija „Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui dėl ES saugumo sąjungos strategijos“. (2020). Žiūrėta gruodžio 1 d. https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:52020DC0605&from=EN
8. Europos Komisija „Pasiūlymas Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami tam tikri sąjungos teisėkūros procedūros, priimami aktai“ 2021 balandžio 21 d. 206 galutinis. Žiūrėta 2021 m. gruodžio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

9. Europos Komisija „Pasiūlymas Tarybos sprendimas kuriuo, atsižvelgiant į Europos Sąjungos interesus, valstybės narės įgaliojamos ratifikuoti Protokolą, kuriuo iš dalies keičiama Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108)“ Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:52018PC0451&from=LT

10. Europos Komisija „Priedas prie Komisijos komunikato Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui Europos požiūrio į dirbtinį intelektą formavimas“ *EUR-Lex*, 2021 m. balandžio 25 d., 237 galutinis. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2018:237:FIN

11. Europos Komisija, „Feasibility study on a forecasting and early warning tool for migration based on artificial intelligence technology“ Europos Sąjungos leidinių biuras Ecorys, 2021 m. vasario 15 d. Žiūrėta 2021 m. gruodžio 1 d. https://op.europa.eu/lt/publication-detail/-/publication/5afa29f0-700a-11eb-9ac9-01aa75ed71a1/language-en/format-PDF/source-191372680

12. Europos Komisija, „Pasiūlymas Europos Parlamento ir Tarybos reglamentas dėl Europos duomenų valdymo, duomenų valdymo aktas“, *Publications Office of the European Union*, 767 galutinis, 2020 m. lapkričio 25 d. Žiūrėta 2021 m. gruodžio 1 d. https://beta.op.europa.eu/en/publication-detail/-/publication/af8cb47b-2f13-11eb-b27b-01aa75ed71a1/language-lt/format-PDF

13. Europos komisija. „Komisija komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ 2021 m. balandžio 29 d. 205 galutinis. Žiūrėta 2021 m. gruodžio 1 d. https://data.consilium.europa.eu/doc/document/ST-8334-2021-INIT/lt/pdf

14. Europos Parlamentas „Pranešimas su rekomendacijomis Komisijai dėl dirbtinio intelekto taikomų civilinės teisės nuostatų“, 2020 m. spalio 10 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_LT.html

15. Europos Parlamentas, „Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų“. Žiūrėta 2021 m. gruodžio 1 d., https://www.europarl.europa.eu/doceo/document/A-8-2017-0005_LT.html

16. Europos Parlamento ir Tarybos direktyva „dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių), 2002 m. liepos 12 d. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32002L0058&from=LT

17. Europos Sąjunga „Europos Parlamento ir Tarybos direktyva dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas“ 2016 m. balandžio 27 d. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016L0680&from=LT

18. Europos Sąjunga „Europos Sąjungos pagrindinių teisių chartija“, *EUR-Lex,* 2016 m. spalio 17 d. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:12016P/TXT&from=LT

19. Europos Sąjunga „Sutartis dėl Europos Sąjungos veikimo suvestinė redakcija“ *Eur-Lex.* Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/ALL/?uri=CELEX%3A12012E%2FTXT

20. Europos Sąjunga, „Europos Parlamento ir Tarybos reglamentas dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“ 2016 m. balandžio 27 d. Žiūrėta 2021 m. gruodžio 1 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:32016R0679&from=LT

21. Europos Sąjungos Taryba, „Tarybos išvados dėl vidaus saugumo ir Europos policijos partnerystės“, 2020 m. lapkričio 24 d. Žiūrėta gruodžio 1 d. https://www.consilium.europa.eu/lt/press/press-releases/2020/12/14/internal-security-council-adopts-conclusions-to-strengthen-cooperation/

22. Europos Sąjungos Taryba, „Komisijos komunikatas Europos parlamentui, tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui. Europos požiūrio į dirbtinį intelektą formavimas“ *EUR-Lex,* 2021 m. balandžio 22 d. 205 galutinis. Žiūrėta 2021 m. gruodžio 1 d. https://data.consilium.europa.eu/doc/document/ST-8334-2021-INIT/lt/pdf

23. Europos Sąjungos Taryba, „Pagrindinių teisių chartija dirbtinio intelekto ir skaitmeninių pokyčių kontekste“ 2020 m. spalio 21 d. Žiūrėta 2021m. gruodžio 1 d. https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/lt/pdf

24. Lietuvos Respublikos švietimo, mokslo ir sporto ministro įsakymas Nr. V-871 „Asmens teisių įgyvendinimo iššūkiai moderniojo visuomenėje: naujų ir besikeičiančių teisių dilemos“. 2021 m. gegužės 25 d. Žiūrėta gruodžio 1 d. https://www.smm.lt/uploads/documents/mokslas/tarptautinis_bendradarbiavimas/LSMC%20TI%20Ilgalaike%20programa%20Asmens%20teises.pdf

25. Nutarimas „Dėl valstybės sienos ženklų, ženklinančių Lietuvos Respublikos sieną sausumoje ir pasienio vandenyse, formos, dydžio nustatymo ir jų statymo tvarkos aprašo

patvirtinimo“, *Lietuvos Respublikos vyriausybė, Valstybės žinios*, 2007 m. kovo 21 d. Nr. 44-16. Žiūrėta 2021 m. gruodžio 1 d. https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.295850/asr

Kiti šaltiniai:

1. „Artificial Intelligence & Human Rights“. *Opportunities & Risks.* 2020 m. lapkričio 15 d. Žiūrėta 2021 m. gruodžio 1 d. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344

2. „Europos Komisija siūlo naujas su kompetencija ir pasitikėjimu dirbtiniu intelektu susijusias taisykles ir veiksmus“ *Teise.Pro* 2021 m. kovo 21 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.teise.pro/index.php/2021/04/21/ek-siulo-naujas-su-kompetencija-ir-pasitikejimu-dirbtiniu-intelektu-susijusias-taisykles-ir-veiksmus/

3. „Journal of Computer Engineering (IOSR-JCE)“ *IOSR*, 2015 m. gegužės 31 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.iosrjournals.org/#school-overview

4. „Journal of Law & Technology“, *AI Time Popular Articles*, 2020 m. sausio 9 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.ijsr.net/gettop10count.php

5. „Lietuva po COVID-19: investicijos, kurios keis ekonomikos DNR“ *Mano vyriausybė* 2020 m. gegužės 15 d. Žiūrėta gruodžio 1 d., https://lrv.lt/lt/naujienos/lietuva-po-covid-19-investicijos-kurios-keis-ekonomikos-dnr

6. „Modernisation of the Data Protection „Convention 108“, Council of Europe, 2018 m. sausio 28 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet?desktop=true

7. „Now Human Rights in the Age of Artificial Intelligence“, *Accessnow*, 2018 m. lapkričio 2 d. Žiūrėta gruodžio 1 d. https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf

8. „What is artificial intelligence and how is it used?“, *Europen Parliament News*, 2021 m. kovo 29 d. Žiūrėta gruodžio 1 d. https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used

9. Benedicto, Ainhoa Ruiz, Akkerman, Mark Akkerman, ir Brunet, Pere, „A Walled World: Towards a global apartheid” *Report, Transnational Institute*, 2020 m. lapkričio 18 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.tni.org/en/walledworld

10. Budreikienė, Jovita ir Grinkevičius, Paulius, „Lietuvos startuoliai šiemet pritraukė 420 mln. Eur investicijų“ *Verso žinios,* 2021 m. spalio 29 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.vz.lt/inovacijos/2021/10/29/lietuvos-startuoliai-siemet-pritrauke-420-mln-eur-investiciju

11. C. Scot, James, „How certain schemes to improve the human condition have failed", *Yale university Press*, 2008 m. vasario 2 d. Žiūrėta 2021 m. gruodžio 1 d. https://politicalscience.yale.edu/publications/seeing-state-how-certain-schemes-improve-human-condition-have-failed

12. Elijus Čivilis ir kt., „Lietuvos dirbtinio intelekto strategija. Ateities vizija", *Ekonomikos ir inovacijų ministerija,* 2019 m. kovo 8 d. Žiūrėta 2021 m. gruodžio 1 d. https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf

13. Europos Parlamentas „Pasiūlymas Dėl dirbtinio intelekto baudžiamojoje teisėje ir jo naudojimo policijoje ir teisminėse institucijose baudžiamosiose bylose". Žiūrėta 2021 m. gruodžio 1 d. https://www.europarl.europa.eu/doceo/document/LIBE-PR-652625_LT.pdf

14. Greg Hullender „Asimov's Centennial: Eight Stories September 1941-April 1943" *Featured Futures.* Žiūrėta 2021 m. gruodžio 1 d., https://featuredfutures.wordpress.com/2020/02/10/asimovs-centennial-eight-stories-september-1941-april-1943/

15. Kate Crowford, „Time to regulate AI that interprets human emotions", *Nature,* 2021 m. balandžio 6 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.nature.com/articles/d41586-021-00868-5

16. Mckinsey&Company „Want to improve consumer experience?" *Collaborate to builda a product data standard*. 2020 balandžio 15 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/want-to-improve-consumer-experience-collaborate-to-build-a-product-data-standard

17. Murauskas Donatas „Dirbtinio intelekto metodai teisės taikymo srityje – galimybes varžo etiniai klausimai" *Vilniaus universiteto „Spektrum"* 2019 lapkričio 11 d. Žiūrėta 2021 m. gruodžio 1 d., https://naujienos.vu.lt/dirbtinio-intelekto-metodai-teises-taikymo-srityje-galimybes-varzo-etiniai-klausimai/

18. Schneier, Bruce „The Public-Private Suveillance Partnership", *The Atlantic,* 2013 m. lapkričio 8 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.theatlantic.com/technology/archive/2013/11/a-fraying-of-the-public-private-surveillance-partnership/281289/

19. Shachar, Ayelet, „Borders in the Time of COVID-19", *Ethics and International Affairs*, 2020 m. kovo 8 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.ethicsandinternationalaffairs.org/2020/borders-in-the-time-of-covid-19/

20. Swatilekha Chakraborty, Rishabh Bhojwani „Artifical intelligence and human rights: Are they convergent parallel to each other? Protesta" 2018 m. gruodžio 22 d. Žiūrėta 2021 m. gruodžio 1 d.

https://repository.ucatolica.edu.co/jspui/bitstream/10983/16334/1/Artificial%20intelligence%20and%20human%20right.pdf

21. The Royal Society. „*Machine learning requires careful stewardship says“* 2017 m. balandžio 25 d. Žiūrėta 2021 m. gruodžio 1 d. https://royalsociety.org/news/2017/04/machine-learning-requires-careful-stewardship-says-royal-society/

22. Zolberg, Arsitide R., „Managing a world on the move”, Population and Development Review, 2006 m. liepos 15 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.jstor.org/stable/20058950

Moksliniai šaltiniai:

1. „Artificial Intelligence and Robotics for Law Enforcement“, *United Nations Interregional Crime and Justice Research Institute (UNICRI) and International Criminal Police Organization (INTERPOL),* 1/1 (2019) 23 – 26. Žiūrėta 2021 m. gruodžio 1 d. http://www.unicri.it/artificial-intelligence-and-robotics-law-enforcement,

2. „Artificial Intelligence Predictive Policing: Efficient, or Unfair“ *Security Distillery*. Žiūrėta 2021 m. gruodžio 1 d. https://thesecuritydistillery.org/all-articles/ethics-artificial-intelligence-and-predictive-policing

3. „Artificial Intelligence, Robotics, Privacy and Data Protection“, *International privacy conference*. 2016 spalio 5 d. Žiūrėta 2021 m. gruodžio 1 d., https://edps.europa.eu/sites/edp/files/publication/16-10-19_marrakesh_ai_paper_en.pdf

4. „Committee of Experts on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence” *Council of Europe*. 2019 m. kovo 19 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.coe.int/en/web/freedom-expression/-/committee-of-experts-on-human-rights-dimensions-of-automated-data-processing-meets-in-strasbourg-for-the-third-time

5. „Discrimination in data-supported decision making” *European Union Agency for Fundamental Rights* (2018) 1/1, 6-8. Žiūrėta 2021 m. gruodžio 1 d. https://fra.europa.eu/en/publication/2018/bigdata-discrimination-data-supported-decision-making

6. „How Artificial Intelligence In Policing Helps Crime Detection“ *INNEFU,* 2021 m. vasario 1 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.innefu.com/blog/how-artificial-intelligence-in-policing-helps-crime-detection

7. „Study on the Human Rights Dimensions of Automated Data Processing Techniques (in Particular Algorithms) and Possible Regulatory Implications“ *The Committee of Experts on Internet Intermediaries* 1/1 (2017): 36-48. Žiūrėta 2021 m. gruodžio 1 d. https://rm.coe.int/study-hr-dimension-of-automateddata-processing-incl-algorithms/168075b94a

8. Alabarce, Miquel Garrich ir Marino, Pablo Pavon, „Artificial intelligence (AI) methods in optical networks“ *Optical Switching and Networking,* 1/1, (2018): 43-57. Žiūrėta 2021 m. gruodžio 1 d. https://doi.org/10.1016/j.osn.2017.12.006

9. Angwin, Julia, Larson, Jetf, Mattu, Surya ir Kirchner, Lauren „Machine Bias“ *ProPublica*. 2016 m. gegužės 23 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

10. Asaro, Peter M., „AI Ethics in Predictive Policing: From Models of Threat to an Ethics of Care“ *IEEE Technology and Society Magazine*. 2019 m. rugsėjo 28 d. Žiūrėta 2021 m. gruodžio 1 d. https://ieeexplore.ieee.org/document/8733937

11. Castrounis, Alex „Brief history of artificial intelligence.“ 1/1 (2020): 1. Žiūrėta 2021 m. gruodžio 1 d. https://www.psdtolive.com/the-history-of-artificial-intelligence/

12. Ciancaglini, Vincenzo, Gibson, Craig ir Sacho, David, „Malicious Uses and Abuses of Artificial Intelligence“ *UNICRI Trend Micro,* 2020 m. lapkričio 19 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence

13. Danišauskas, Gintautas, „Teisėsaugos funkcijų vykdančių institucijų rūšys bei teismo vieta šių institucijų sistemoje“ ISSN 2029–2244, (2009) 2-14. Žiūrėta 2021 m. gruodžio 1 d. https://ojs.mruni.eu/ojs/societal-studies/article/download/1415/1356

14. Galeon, Dom, „Softbank CEO: The Singularity Will Happen by“ 1/1 (2017): 1. Žiūrėta 2021 m. gruodžio 1 d. https://futurism.com/softbank-ceo-the-singularity-will-happen-by-2047

15. Gonzalez, Fuster, „AI and law enforcement: Impact on fundamental rights“, European Parliament ThinkTank, 2020 m. liepos 7 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf

16. Jenkins, Rayn ir Purves, Duncan „Artificial Intelligence and Predictive Policing: A Roadmap for Research“ *Ethics+Emerging Sienses Group,* 2020 m. rugsėjo 30 d. Žiūrėta 2021 m. gruodžio 1 d. http://aipolicing.org/year-1-report.pdf,

17. Kuconis, Pranas ir Nekrošius Vytautas, *Teisėsaugos institucijos*. „Justitia“ (2001)

18. Leese, Matthias, „Predictive Policing: Proceed, but with Care“, *Policy Perspectives* 2020 m. gruodžio 6 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.researchgate.net/publication/347443927_Predictive_Policing_Proceed_but_with_Care

19. Mills, Michael, *„Artificial intelligence in law: the state of play 2016“,* 1/1 (2016): 1-6. Žiūrėta 2021 m. gruodžio 1 d. https://www.neotalogic.com/wp-content/uploads/2016/04/Artificial-Intelligence-in-Law-The-State-of-Play-2016.pdf

20. Rigano, Christopher „Using Artificial Intelligence to Address Criminal Justice Needs“ *National Institute of Justice Journal* 2019 m. sausio 17 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.ojp.gov/pdffiles1/nij/252038.pdf

21. Rudin, Cynthia, „Predictive Policing: Using Machine Learning to Detect Patterns of Crime“, *Wired,* 2021 m. liepos 2 d. Žiūrėta 2021 m. gruodžio 1 d. https://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime/

22. Stone, Peter, Brooks, Rodney, Brynjolfsson, Erik, Calo Ryan, Etzioni, Oren, Hager Greg, „Artificial Intelligence and life in 2030“ *Stanford University,* 1/1 (2016): 4-16. Žiūrėta 2021 m. gruodžio 1 d. https://apo.org.au/sites/default/files/resource-files/2016-09/apo-nid210721.pdf

23. Susskind, Richard. *„The End Of Lawyers? Rethinking The Nature Of Legal* Services“ 1/1 (2010): 25-49. Žiūrėta 2021 m. gruodžio 1 d. https://www.goodreads.com/book/show/3075321-the-end-of-lawyers

24. Visockas, Evaldas, „Pasitikėjimas teisėsaugos institucijomis Lietuvoje*“ Teisės problemos,* 2/2 (2016): 93-107, https://teise.org/wp-content/uploads/2017/02/Visockas-2016-2.pdf

Specialioji literatūra:

1. Gaižauskaitė, Inga ir Valavičinė, Natalija, „Socialinių tyrimų metodai Kokybinis tyrimas“ Vilnius (2016): 35-38. Žiūrėta 2021 m. gruodžio 1 d.

2. Davies, Malcolm, Croall, Hazel ir Tyrer, Jame, „An Introduction to the Criminal Justice System in England and Wales. Pearson Education“, *Ursula Smartt* 1/1 (2006): 62-71. Žiūrėta 2021 m. gruodžio 1 d. https://books.google.lt/books?id=X4j2iLrstToC&pg=PA32&dq=Davies+M.;+Croall,+H.;+Tyrer,+J.+Criminal+Justice+%E2%80%93+An+Introduction+to+the+Criminal+Justice+System+in+England+and+Wales.+Pearson+Education,+2005.&hl=lt&sa=X&ved=2ahUKEwiTtZrCgMv0AhVSQfEDHUNCBo4Q6AF6BAgKEAI#v=onepage&q&f=false

3. Merkevičius, Remigijus, „Baudžiamajame procese atsitiktinai gautos faktinės informacijos panaudojimas kitame baudžiamajame procese“, *Lietuvos Respublikos Baudžiamajam kodeksui - 10 metų.* Žiūrėta 201 m. gruodžio 1 d. https://www.lituanistika.lt/content/41729

4. Minsky, Marvin, „The Emotion Machine“ *Simon & Schuster*, 1/1 (2007): 3-7. Žiūrėta 2021 m. gruodžio 1 d. https://www.simonandschuster.com/books/The-Emotion-Machine/Marvin-Minsky/9780743276641

5. Rupšienė, Liudmila, „Kokybinio tyrimo duomenų rinkimo metodologija“. *Klaipėdos universitetas*, 2007 m. sausio 8 d. 63-75. Žiūrėta 2021 m. gruodžio 1 d. https://www.researchgate.net/publication/323497804_Kokybiniu_tyrimu_duomenu_rinkimo_metodologija

6. Tidikis, Rimantas „Socialinių mokslų tyrimų metodologija“, *Lietuvos teisės universitetas*, (2003): 41-56. Žiūrėta 2021 m. gruodžio 1 d. https://repository.mruni.eu/handle/007/15459?show=full

7. Todorov, Alexander „Face value: The irresistible influence of first impressions“, *Princeton University Press*, 2017 m. birželio 6 d. Žiūrėta 2021 m. gruodžio 1 d., https://press.princeton.edu/books/hardcover/9780691167497/face-value

8. Wischmeyer, Thomas ir Rademacher, Timo, „Regulating artificial intelligence“ *Springer* 1/1, (2020): 307-321. Žiūrėta 2021 m. gruodžio 1 d. *https://books.google.lt/books?id=FQ3BDwAAQBAJ&lpg=PA307&ots=f2eVC4HnCr&dq=Artificial%20intelligence%20and%20healthcare%3A%20procedures.%20In%3A%20T.%20Wischmeyer%20and%20%20T.%20Rademacher&hl=lt&pg=PA307#v=onepage&q&f=false*

PRIEDAI:

Priedas Nr. 1. Interviu metu užduoti klausimai civiliam technologams (ekspertams).

Laba diena,

Esu Kornelijus Zakaras, šiuo metu studijuoju Mykolo Romerio universitete Viešojo saugumo akademijoje, rašau Magistro baigiamąjį darbą. Mano MBD tema „Dirbtinio intelekto naudojimo teisėsaugos institucijų veikloje iššūkiai žmogaus teisių požiūriu“.
Magistro baigiamajame darbe atlieku kokybinį tyrimą – atlieku ekspertų ir pareigūnų apklausą. Planuoju apklausti 3-4 ekspertus ir 3-4 pareigūnus. Jus pasirinkau vienu iš jų. Darbe respondentų tapatybė nebus atskleista, ekspertai bus įvardinti kaip ekspertai E1, E2, ir t.t., pareigūnai bus įvardinti kaip P1, P2, ir t.t.

Prašau užpildyti anketą, atsakant į atviro pobūdžio klausimus.

1. Kaip, Jūsų nuomone, dirbtinis intelektas palengvino mūsų visų viešąjį ir privatų gyvenimą? Kokias svarbiausias problemas jis išsprendė? Kaip manote, kokios problemos bus išspręstos ateityje?
2. Kaip manote, ar dirbtinio intelekto technologijos su Konstitucijoje numatytomis teisės normomis neprasilenkia? Pvz. teise į asmens privatų gyvenimą. Jei taip, tai kodėl?
3. Kaip manote, ar gauti duomenys pasitelkiant dirbtinio intelekto sistemas, yra neviešo pobūdžio? Kokia gali būti sistemos kūrėjo atsakomybė už gautų duomenų išviešinimą?
4. Ar Jūsų manymu institucijos, leidžiančios sistemų kūrėjams gauti prieigą prie informacijos, užtikrins, kad informacija būtų naudojama pagal paskirtį? Ar yra galimybė vykdyti atvirą šios informacijos stebėjimą ar kontrolę?
5. Kalbant apie dirbtinį intelektą dažnai iškeliamas duomenų apsaugos privatumo klausimas. Tokios dirbtinio intelekto technologijos, kaip veido atpažinimo sistemos, yra laikomos į privatumą besibraunančia technologija. Kaip manote, ar galima rasti balansą tarp technologijų plėtros ir duomenų apsaugos?
6. Ar dirbtinio intelekto sistema teikia naudos visuomenės saugumui? Ar taikomi metodai yra pranašesni už kitus tradicinius teisėsaugos institucijų metodus?
7. Kokios Jums žinomos dirbtinio intelekto technologijos yra labiausiai pasiteisinusios? (Teisėsaugos institucijose, medicinos srityje, transporto logistikoje).
8. Kas, Jūsų nuomone, nutiks, kai teisėsaugos institucijose naudojama dirbtinio intelekto sistema padarys klaidą?
9. Kaip manote, į kurią dirbtinio intelekto technologijų pusę turėtų būti nukreipti tyrimai ir inovacijos? Kokie tyrimai ar inovacijos Jums įdomiausios?
10. Kaip vertinate lietuvių pasiekimus dirbtinio intelekto srityse?

Ačiū už pateiktus atsakymus!

Priedas Nr. 2. Interviu metu užduoti klausimai teisėsaugos institucijų pareigūnams.

Laba diena,

Esu Kornelijus Zakaras, šiuo metu studijuoju Mykolo Romerio universitete Viešojo saugumo akademijoje, rašau Magistro baigiamąjį darbą. Mano MBD tema „Dirbtinio intelekto naudojimo teisėsaugos institucijų veikloje iššūkiai žmogaus teisių požiūriu“.
Magistro baigiamajame darbe atlieku kokybinį tyrimą – atlieku ekspertų ir pareigūnų apklausą. Planuoju apklausti 3-4 ekspertus ir 3-4 pareigūnus. Jus pasirinkau vienu iš jų. Darbe respondentų tapatybė nebus atskleista, ekspertai bus įvardinti kaip ekspertai E1, E2, ir t.t., pareigūnai bus įvardinti kaip P1, P2, ir t.t.

Prašau užpildyti anketą, atsakant į atviro pobūdžio klausimus.

1. Kaip, Jūsų nuomone, dirbtinis intelektas palengvino mūsų visų viešąjį ir privatų gyvenimą? Kokias svarbiausias problemas jis išsprendė? Kaip manote, kokios problemos bus išspręstos ateityje?
2. Kalbant apie dirbtinį intelektą dažnai iškeliamas duomenų apsaugos ir privatumo klausimas. Tokios dirbtinio intelekto technologijos, kaip veido atpažinimo sistemos, yra laikomos į privatumą besibraunančia technologija. Kaip manote, ar galima rasti balansą tarp technologijų plėtros ir duomenų apsaugos?
3. Ar dirbtinio intelekto sistema teikia naudos visuomenės saugumui? Ar taikomi metodai yra pranašesni už kitus tradicinius teisėsaugos institucijų metodus?
4. Kaip, Jūsų manymu, pareigūnai gali pritaikyti dirbtinio intelekto pagrindu gautus sistemos rezultatus, pvz. modeliuojant būsimas grėsmes, kuriant rizikos profilius, nustatant tam tikrus algoritmus?
5. Kaip manote, ar pakanka teisės aktų, kurie reglamentuoja teisėtą ir efektyvų dirbtinio intelekto technologijų taikymą teisėsaugos institucijose?
6. Kokias žinote dirbtinio intelekto pagrindu veikiančias sistemas teisėsaugos institucijose? Kokios, Jūsų manymų, labiausiai pasiteisinusios dirbtinio intelekto pagrindu veikiančios technologijų sistemos teisėsaugos institucijose? Pvz. „HERTA“ - veido atpažinimo sistema, „D4FLY“ - tapatybės ir dokumentų klastojimo nustatymas keliaujant, „PoliScan FM1“ - greičio matavimo prietaisai (trikojai), „Bloomberg“ - veido atpažinimo sistema.
7. Kas, Jūsų nuomone, nutiks, kai teisėsaugos institucijose naudojama dirbtinio intelekto sistema padarys klaidą?
8. Kaip manote, kokie dirbtinio intelekto inovacijos yra perspektyviausios kalbant apie visuomenės saugumo užtikrinimą?

Ačiū už pateiktus atsakymus!

Priedas Nr. 3 Transkribuotas interviu atsakymas teisėsaugos pareigūno. *(tekstas nekoreguotas, netaisytas).*

Pirmas klausimas: ***Kaip, Jūsų nuomone, dirbtinis intelektas palengvino mūsų visų viešąjį ir privatų gyvenimą? Kokias svarbiausias problemas jis išsprendė? Kaip manote, kokios problemos bus išspręstos ateityje?***

Iš „Google“ paieškos sistemos vieną kartą sumažinus kažkokią paiešką, paskui daugybę kartų „Google“ Kad krypsta ta pačia kryptimi, nors stogo visai nereikia. Čia mes pastebime, bet yra truputį daugybė vietų, kur mes net nežinome, kas mus kreipia. Tam tikra tam tikrų paslaugų, tam tikrų prekių, tam tikrų straipsnių kryptimi. Pagal mums nežinomos taisyklės, ir tokiu būdu ji nu jeigu mes nežiūrėsime blaiviai, tai jeigu neužduosime sau klausimo, kodėl mane ten kreipia, tai mūsų žinojimo. Mūsų veiklos kryptis, dirbtinis intelektas pradės formuoti, pradeda formuoti, o ne tik siūlo sprendimus. Antras dalykas yra kiti tyrimai su Londono taksistais ir GPS, kad kai mums nebereikia priimti sprendimų, pavyzdžiui, mes nebemokame skaičiuoti automatiškai, mintinai arba nesigaudome miestuose. Bet ši pjesė - tai kaip mums taip, kaip tikras, tam tikras funkcijas atiduoti apdirbti intelektui. Tai mūsų smegenys tas vietas praranda, nes prarandame tuos gebėjimus tai ir ta kryptimi. Turbūt kadangi duomenų vis daugės, laikas turbūt vis greitėjantis. Tai tos problemos, jos iš vienos pusės, bus sprendžiamos. Iš kitos pusės atsiras naujos, sukuriamos to paties mūsų naudojimosi dirbtinis intelektas. Supratau ačiū.

Antras klausimas: ***Kalbant apie dirbtinį intelektą dažnai iškeliamas duomenų apsaugos ir privatumo klausimas. Tokios dirbtinio intelekto technologijos, kaip veido atpažinimo sistemos, yra laikomos į privatumą besibraunančia technologija. Kaip manote, ar galima rasti balansą tarp technologijų plėtros ir duomenų apsaugos?***

Nu balanso turbūt visą laiką reikia ieškoti. Ar jį galima tikrai pilnai surasti? Tai sunku atsakyti žiūrint vėl kokioje srityje. Mes kalbėsime iš vienos pusės. Mes norime, kad, mūsų duomenimis, teisėtai naudotųsi įvairios institucijos arba naudotųsi tik ta kryptimi, kuria mes jomis joms leidžiame. Bet iš kitos pusės, mes patys sakau elektroninėje erdvėje labai plačiai siejame savo visokius duomenis nuo to, ką mėgstame valgyti iki to, ką perkame, ir panašiai. Tai pirmiausia mes patys turime saugoti savo privatumą. O tai, ką su mūsų duomenimis daro institucijos, vis dėlto yra įmanoma patikrinti. Man paskambino truputį pašto prekes išsiimti. Taip, aš skambinau dėl to čia dabar interviu turime patys saugoti savo privatumą. O institucijos, kurioje dirba su asmens duomenimis, tai jos egzistuoja taisyklės, ir visi tie dirbtiniai intelektai, tos taisyklės ten yra sudedamos jos yra parašytos. Darbas su jumis aprašytas. Tai, ką daro institucijos su mums su mūsų duomenimis. Tai jau bent galima atsekti, patikrinti ir, reikalui esant, netgi prieštarauti arba paprašyti pasiaiškinti. <Nu> pats pilietis gali tą padaryti. Tai o tą balansą tarp duomenų apsaugos ir technologijų plėtros mums <nu> nu kitaip. Mes tiesiog

negalime, kaip mes radome balansą tarp pėsčiųjų ir automobilių, ir tarp kitų dalykų. Taip turėsime ir šitoje vietoj surasti, nes gyvenimas vystosi ta kryptimi ir niekur nepabėgsi. Ačiū.

Trečias klausimas: ***Ar dirbtinio intelekto sistema teikia naudos visuomenės saugumui? Ar taikomi metodai yra pranašesni už kitus tradicinius teisėsaugos institucijų metodus?***

Gali teikti visuomenės saugumui naudos. Tinkamai naudojama tikrai gali teikti visuomenės saugumui naudos tiek, kiek gali iš viso institucijos užtikrinti visuomenės saugumą. Nes jeigu mes tuo kalbėtumėme plačiąja prasme, tai pirmiausia pats individas turėtų rūpintis savo duomenis, duomenų sauga ir savo paties saugumu, savo sveikata ir t. t.. Bet visų valstybinės institucijos teisėsaugos institucijose tikrai gali ir gauna, ir gali gauti didelę pagalbą iš informacinių technologijų, iš dirbtinio intelekto, tame tarpe, nes žmonių tose institucijose pareigūnų, nėra perspektyvų, kad jų daugėtų, o domenus tai jie tikrai visą laiką didėja ir prekių judėjimas, asmenų judėjimas. Jis visada intensyviai ir turbūt eis ta kryptimi toliau. Reiškia, mums reikės apdoroti vis daugiau ir daugiau duomenų, bandant iš to didžiulio kiekio atsirinkti tuos atvejus, kuriuos reikia patikrinti ir fiziškai prižiūrėti, fiziškai ir tikrai įsitikinti, ar ten yra pasikėsinimai pažeisti pažeidimai, ar panašūs visuomenę kenkiantys dalykai.

Ačiū.

Ketvirtas klausimas: ***Kaip, Jūsų manymu, pareigūnai gali pritaikyti dirbtinio intelekto pagrindu gautus sistemos rezultatus, pvz. modeliuojant būsimas grėsmes, kuriant rizikos profilius, nustatant tam tikrus algoritmus?***

Tai iš dirbtinio intelekto, kuriose dirbtinį intelektą reikia sukrauti tam tikrus algoritmus. Tada dirbtinis intelektas apdoroja pagal tuos algoritmus įvairius duomenis, įvairių duomenų srautus. Jisai pasiūlys išvadą arba sprendimą. Ta išvada: jeigu mes paprastai taip ir programuojame dirbtinį intelektą, kad jis išvadą rodytų tam tikros rizikos buvimą, o toliau mes jau turime fiziškai įsitikinti, iš tikrųjų egzistuoja. Rizika neegzistuoja. Taip, ir tas intelektas mums gali padėti. Nu grėsmė.

Rizika - tai beveik tas pats toliau balanso turbūt visą laiką reikia ieškoti. Ar jį galima tikrai pilnai surasti? Tai sunku atsakyti žiūrint vėl kokioje srityje. Mes kalbėsime iš vienos pusės. Mes norime, kad, mūsų duomenimis, teisėtai naudotųsi įvairios institucijos arba naudotųsi tik tą apimtimi, kuria mes joms leidžiame. Bet iš kitos pusės, mes patys sakau elektroninėje erdvėje labai plačiai siejame savo visokius duomenis nuo to, ką mėgstame valgyti iki to, ką perkame, ir panašiai. Tai pirmiausia mes patys turime saugoti savo privatumą. O tai, ką su mūsų duomenimis daro institucijos, vis dėlto yra įmanoma patikrinti. Man paskambino truputį pašto prekes išsiimti. Taip patys saugoti savo privatumą. O institucijos, kurioje dirba su asmens duomenimis, tai jos egzistuoja taisyklės, ir visi tie dirbtiniai intelektai, tos taisyklės ten yra sudedamos jos yra

parašytos. Darbas su jumis aprašytas. Tai, ką daro institucijos su mums su mūsų duomenimis. Tai jau bent galima atsekti, patikrinti ir, reikalui esant, netgi prieštarauti arba paprašyti pasiaiškinti. pats pilietis gali tą padaryti. Tai o tą balansą tarp duomenų apsaugos ir technologijų plėtros mums nu kitaip. Mes tiesiog negalime, kaip mes radome balansą tarp pėsčiųjų ir automobilių, ir tarp kitų dalykų. Taip turėsime ir šitoje vietoj surasti, nes gyvenimas vystosi ta kryptimi ir niekur nepabėgsi.

Tai iš dirbtinio intelekto, kuriose dirbtinį intelektą reikia sukrauti tam tikrus algoritmus. Tada dirbtinis intelektas apdoroja pagal tuos algoritmus įvairius duomenis, įvairių duomenų srautus. Jisai pasiūlys išvadą arba sprendimą. Ta išvada: jeigu mes paprastai taip ir programuojame dirbtinį intelektą, kad išvadą rodytų tam tikros rizikos buvimą, o toliau mes jau turime fiziškai įsitikinti, iš tikrųjų egzistuoja. Rizika neegzistuoja. Taip, ir tas intelektas mums gali padėti. Nu grėsmė. Tikrinti, ar tai yra taip įsitikinęs. Tada žmogus galėtų nuspręsti: jeigu tirtis ar intelektas parinko neteisingai, tai tada galbūt neteisingi duomenys arba neteisingai algoritmai, ir tada tą dirbtinio intelekto jį patį galima tobulinti, kad kitą kartą jisai parodytų tiksliau, tai čia yra visi visą laiką, niekada nesibaigiantis procesas. Tarpo žmogaus, kuris naudojasi dirbtinio intelekto rezultatais tarp žmogaus, kuris tą dirbtinį intelektą palaiko ir ir aprūpina duomenimis ar taisyklėmis ir telpa tarp nu tarptų, tarp tų pačių duomenų. Be abejo, katinų dirbtinis intelektas yra labai geras tuo, kad jisai gali greitai ir nepavargdamas, bet kuriuo paros metu apdoroti didžiulius duomenų kiekius. O rezultatas priklausys nuo to, ką ko tu jį pašėrei ir kaip tu paskui įsitikinai. Ar jisai tikrai pastebėjau tą neatitikimą, riziką? Ar jisai suklydo? Ačiū.

Penktas klausimas: ***Kaip manote, ar pakanka teisės aktų, kurie reglamentuoja teisėtą ir efektyvų dirbtinio intelekto technologijų taikymą teisėsaugos institucijose?***

Labai sunku pasakyti, ar pakanka, nes čia vėl ratus yra bandoma. Turėtų būti bandoma surasti balansą. Ką leisti dirbtiniam intelektui ir ko jam neleisti. Bet jeigu mes jiems viską ribosime, tai tada rezultatą atitinkamai turėsime. Nu, labai netikslūs. Dabar taip atsitinka, kad technologijos vystosi greičiau negu visuomenė negu mūsų supratimas apie ją negu mūsų mokėjimas jomis naudotis ir t. t.. Tai gaunasi, kad teisės aktai. Jie eina iš paskos pažangos, ir daugeliu atvejų nuėjau tiesiog tobulai parašyti neįmanoma, ir jie visada vėluos. Juk galų gale, visose kitose srityse mes reiškia reglamentuojame kažkokią, pavyzdžiui, sankcijas arba, arba bausmes, arba kažką. Po to, kai jau žinome, kad tokie dalykai vyksta, tai mes negalime iš anksto nuspėti, kad taip bus, tai tas reglamentavimas. Jisai šitoje srityje tikrai yra labai sudėtingas. Reikia labai turėti specialių žinių ir negali reglamentavimas virsti apynasriu nuo teisėsaugos institucijų, kad jau nieko negalima, nes reglamentavimas - teisinis riboja teisėsaugos institucijų veiksmus, bet tuo tarpu nelabai riboja visuomenės ir privačių piliečių veiksmų. Mums daug kas

draudžiama daryti dėl to, kad nepažeistume ko noras, o piliečiai? Kol nepaaukoti, tai skaitosi, kad nieko nepažeidė, nors turi visas teises, bet kokiu būdu keistis duomenimis, platinti, daryti tam tikras išvadas iš jų ir tas ir yra daroma, ir padeda tos pačios tos pačios reiškia ir viešuose šaltiniuose esančios įsiūti algoritmai ir technologijos. Teisinis reglamentavimas. Nu, ar jisai yra pakankamas, nelabai sunku pasakyti, bet paprastai tiesiog reglamentavimas seka paskui, paskui metodus, paskui gyvenimą.

O iš darbinės aplinkos, kaip būtent ar pakanka ir nepakanka, būtent kas siejasi su jūsų tiesioginiu darbu? Koks buvo klausimas, kaip susijęs su jūsų darbu, kaip, ar pakanka jūsų darbinėje aplinkoje, teisės aktų ar naudojami naudojant dirbtinį intelektą vis daugiau naudoja dirbtinio intelekto sistemoms, persiųs darbinius ir dirbtinėje aplinkoje.

Na, o dabar yra reikalavimai pagal Bendrąjį asmens duomenų apsaugos reglamentą yra nacionaliniai reklama, tai yra Muitinės departamento, kai nėra tikslus įsakymas. Ten reikia vertinti visą sistemą su tuo asmens duomenų požiūriu, bet jo reikalingumas nu, tiesiog reikia įgyvendinti reglamentą. O pats įsakymas? Ar jisai tai yra papildomas darbas? Kurį reikia atlikti prieš kuriant arba jau sukūrus sistemą. Mes jį atliksime pagal nustatytas taisykles. Bet ar jisai padės, nors iš tikrųjų apsaugoti? Man atrodo, kad labiau yra darbas dėl darbo labiau gaišina, negu padeda. Vakarais skaitydamas atsakinėdamas į klausimus tu apgalvoji tam tikras vietas. Kaip čia reikėtų padaryti, ir čia gerai padaryta, bet nu, gal ir galima sakyti, kad jis kažkiek yra kaip orientyras, kaip. Bet iš tikrųjų kaip dirbti. Tai kaip dirbti. Tai egzistuoja arba turi būti paremtos kitos taisyklės, ir jos jau būtų ne su pačiu dirbtinio intelekto arba su pačia sistema, kurioje jos naudojamos, nepriklausomai nuo to, kokie ten duomenys yra.

Šeštas klausimas: ***Kokias žinote dirbtinio intelekto pagrindu veikiančias sistemas teisėsaugos institucijose? Kokios, Jūsų manymų, labiausiai pasiteisinusios dirbtinio intelekto pagrindu veikiančios technologijų sistemos teisėsaugos institucijose? Pvz. „HERTA“ - veido atpažinimo sistema, „D4FLY“ - tapatybės ir dokumentų klastojimo nustatymas keliaujant, „PoliScan FM1“ - greičio matavimo prietaisai (trikojai), „Bloomberg“ - veido atpažinimo sistema.***

Apie kai kurias iš jų esu girdėjusi ir esu girdėjusi, kad jos dirba gerai ir policijai bent jau yra naudingos. Bet ne, nesu čiupinėjusi dabar mes, pavyzdžiui, mes mūsų neturėjome ir dabar yra tie įrankiai. Tiktai neturime specialistų, kuris su jais dirba. Yra taikyti dirbtinio intelekto metodai. Tikrai tiktai tiek, kad jie pasiteisino tiktai tikrinimui po muitinio įforminimo reiškia iš gyvų duomenų, jau muitinės sukauptų duomenų. Dirbtinis intelektas buvo apmokytas atrasti pažeidimus, kuriuos mes pražiopsojome, ir tada atiduodavo juos ne ūkio subjektų patikrinimo skyriuje, ir jie naudodavo juos atlikdami auditus. Ir tikrai, tie auditai buvo sėkmingi. Ir tikrai tų pažeidimų buvo nustatyta ir ten mokesčiai priskaičiuoti ir panašiai. Tai šitoje vietoj tie įrankiai

buvo sėkmingi. Bet tai buvo dėl to, kad kodėl mes šiandien dar įforminimui, va tam tikrinimui, konkrečiam tikrinimui. Bet konkretaus krovinio, kuris dabar važiuoja, dar nesugeba pritaikyti jokio dirbtinio intelekto. Todėl, kad atsakymo reikia labai greitai ir todėl, kad tam vienam kartui tu turi mažai duomenų. Įsivaizduokime, tu gali, reiškia išanalizavęs reiškia milijoną įrašų, atrasti jame ten, sakykime, aibę nu, sakykime, ten dešimt vienetų, kurie kelia tavo įtarimus, ir, o atlikdamas auditą, kuriam tu turi pakankamai daug laiko, gali tuos atvejus patikrinti ir turbūt ten rasi tuo tarpu įforminimo metu reikia nu s spartos ir arba, pavyzdžiui, aš žinau, kad buvo daryti, bet daryti net ne tiktai Lietuvoje, bet kelių šalių kartu buvo daryti. Bandyta padaryti algoritmus, suprasti, atrasti narkotikus konteineriuose. Buvo surinkta tikrai daugybės duomenų iš kelių šalių jie ten apdoroti - taip, bet pasirodė, kad ta imtis narkotikų konteineriuose, palyginus su visu konteinerių srauto ir visų prekių srautą, yra tokia maža. Nu, kad dirbtinį intelektą yra per mažai duomenų, kad jis galėtų atspėti tiesiog milijoną. Žinau tai kaip adata šieno kupetoje. Tai aš tikiu, kad tokie įrankiai yra geri, galimi, ir mes irgi bandysime pasitelkti tokius įrankius. Nu ne tokius, bet atitinkamus muitinėje reikalingus įrankius kaip tas rentgeno vaizdų atpažinimas, kuriems turėtų pagreitinti darbą labai smarkiai, be to, nu ką, dirbtinis intelektas. Jeigu jame taisyklės yra teisingos, tai visai objektyvus. Negaliu pasakyti, kad tai tuo metu buvo, mirktelėjo. Kai važiavome jisai objektyvią dirbsite. Nereikia nė ne ilsėtis. Neini pamainas keisti. Tai jisai turėtų dirbti greitai, efektyviai, su daug duomenų ir turėtų nurodyti rizikingus atvejus. Bet paskui juos visus vis tiek reikės žmogui patikrinti. Ir koks čia klausimas, labiausiai pasiteisinusius. Nu, pavyzdžiui, veidų. Aš įsivaizduoju, kad tikrai jinai būtų tik tiek, kad muitinėje nedirba su veidais. Muitinėse klientas yra, nu, yra prekės, o ne asmuo. Bet manau, kad dirbtinis intelektas tikrai gali daug geriau atpažinti ir sulyginti veidus, negu tai gali žmogaus akis. Tai tikimės, kad, pavyzdžiui, kokias rentgeno nuotraukas ar netgi, pavyzdžiui, automobilių fotografijos mes apie tai galvojome, kad galbūt internetas, dirbtinis intelektas galėtų sulyginti. Ar čia tas pats automobilis? Ar čia jau kitas tiktai numeris tas pats, pavyzdžiui, tai nu, bandysime tuo keliu eiti. Bet kai pasiseks, bus matyt. Ačiū.

Septintas klausimas: ***Kas, Jūsų nuomone, nutiks, kai teisėsaugos institucijose naudojama dirbtinio intelekto sistema padarys klaidą?***

Aš supratau, supratau, kad tai, kaip aš įsakiau, reiškia nu - dirbtinio intelekto sistema, ne neuždeda antrankių. Jinai tiktai nurodo rizika, o be žmogaus įsikišimo toliau neįvertinsi. Ta rizika yra pasiteisinusi ir nepastatyta. Tai vat aš ir sakau, kad reiškia pirmiausia tai žmogus vis tiek priims galutinį sprendimą. Nu, aš neįsivaizduoju, kad būtų kur nors kokioje sistemoje. Bent jau teisminėje institucijoje, teisėsaugos institucijoje, tikrai nebuvo. Neturi būti ne neįmanoma tokia sistema, kad dirbtinis intelektas priimtų sprendimą. Ar tai galutinis sprendimas? Neįmanoma. Tokia sistema vis tiek yra reiškia. Žmogaus įsikišimas privalomas. Antras dalykas

teisėsaugos institucijoje - tam tikrų atvejų sankcionuotų. Tu tikrai galėsi sužinoti, kodėl dirbtinis intelektas priėmė sprendimą, nes procedūra kokios taisyklės, kaip jos taikomos. Ant kokių duomenų jinai vis tiek turi būti aprašytas ir neturi būti įteisinta. Nebus taip kad aišku, ar aš nežinau, kodėl taip įvyko. Atsiprašome, bet yra daug blogiau. Turbūt su tais dirbtinis intelektas, kurie yra įsiūti visokiose, reiškia programose, Facebook ir dar kažkur, nes mes nežinome, kaip jie veikia ir nes mes nežinome ir nėra ką paduoti į teismą, ir nėra ką apkaltinti mane suklaidinus ten skiepų žalą, pavyzdžiui, arba dar kažkuo, nes tai kelia man atrodo, visuomenės saugumui, visuomenės savarankiškumui ir laisvei tai, ko gero, kelia didesnę grėsmę negu tie dirbtinio intelekto, kurie yra taikomi oficialiai oficialiose teisėtose valstybės institucijose, demokratinėse valstybėse. Tai čia, nu, man atrodo, vienareikšmiškai

Aštuntas klausimas: ***Kaip manote, kokie dirbtinio intelekto inovacijos yra perspektyviausios kalbant apie visuomenės saugumo užtikrinimą?***

Po visokių yra turbūt tų sprendinių, yra visokių ten tų startuolių ir t. t., kurie kuria vis naujas ir naujas, ir ne visada mes jas žinome, nes ne visas spėjome sužinoti. Bet turbūt galima įsivaizduoti, kad galima sukurti dirbtiniu intelektu ir naudingu visuomenei, ir žolininkų visuomenėje. Tai gal mes ne visi ir ne iš karto sugebėsime atskirti tai, kas padeda užtikrinti saugumą ir kas atvirkščiai - nesmagu. Teisėsaugos institucijos jokios irgi eina, eina pagal paskui nustatytus nusikaltimus arba pažeidimus, arba pastebėtas rizikas. Ir tada, kai tų dalykų susikaupia, jos ieško būdų, kaip tą spręsti, ir tokiu būdu pasitelkia dirbtinį intelektą. Bet tam tikri įvykiai prieš tai jau yra įvykę. Taip ir blogybė. Ne tai turbūt ateityje atsiras visokiausių. Nu, yra dabar gi yra visokių ten tos dirbtinės nosys, kurios atpažįsta visokias reiškia medžiagas, narkotines, neranda nenarkotines galima turbūt atpažinti blogietį iš elgesio, iš neverbalinės kalbos. Iš nu, mes bandome dirbti su tais duomenimis, kurie yra sukaupti. Tai turbūt tų visokių sprendimų ateičiai jau tikrai galima. Jų atsiras, kurių mes net neįsivaizduojame, kas gali atsirasti, bet iš kitos pusės auga nu, blogiečiai irgi naudojasi tomis pačiomis technologijomis, ir jie galbūt net naudojasi jomis laisviau, nes, sakykime, valstybinei institucijai, norint kažką įsigyti, reikia pirmiausia gauti pelną, įrodyti, kad to reikia. Paskui trunka kelis metus, kol tas įdiegiama, reiškia, per tą laiką tas pasensta. Tada mes pradedame kažkada taikyti. Tuo tarpu blogąja puse. Jeigu yra pinigų, o pinigų užsidirbame iš tos pačios veiklos, tai jai nereikia skelbti konkurso ir įsikiškite šiltai apsirengti reiškia tai teisinga. Tikėjome, gali įsigyti, jeigu tik turint noro ir pinigų, tai gali įsigyti čia pat ir jau pradėti taikyti tai bet nu, ir dar yra paslėpta pusė, kurios mes nematome, kur aš jau kelis kartus kalbėjau ir apie ką niekas nešneka, kalba apie duomenų apsaugą ir dirbtinį intelektą, bet yra tie dalykai, kurie mums nežinant, formuoja mūsų pasaulėžiūrą. Kas, aš manau, yra tikrai labai blogai, nes mes to net nežinome. Mes matome trikojį ir žinome, kad nufotografavo ir žinome, kad mes viršijame greitį ir panašiai. Mes žinome,

kad nu kažkokios institucijos tam tikra, tam tikra mano veikla tikriausiai domisi, nes mokesčių inspekcija domisi viena. Mano veikla reiškia, nežinau, policija kita, dar kažkas. Trečia, žinai pagal tai, ko ką aš gyvenime veikiu. Bet yra daug sričių, kur mes nežinome, kas mumis domisi ir nežino, bet kai, kaip naudoja, visi mano reiškia pirkimai elektroniniai. Visi visos mano paieškos „Google“. Visi mano asmeniniai laiškai gauti. Jie įtakoja tam tikras kryptis ir sukiojo mano dėmesį, bando atkreipti nupirkti mano dėmesį, nukreipti į tam tikrą lygį. Na, ir jeigu aš nebūsiu budrus, aš ne taip ir manysiu, kad ta kryptis yra vienintelė, nors iš tikrųjų krypčių yra visos pusės. Tai šita pusė visuomenės saugumo, mano rodo, yra gal net svarbesnė už tą, kurią gali už tai užtikrinti institucijos, nes pirmiausia aš turiu pasirūpinti savo saugumo, kiek nuo manęs priklauso, o tik paskui prašyti iš valstybės, kad tam tikrais atvejais mane apsaugotų, apgintų arba nubaustų. Kas mums pakenkė? Daugeliu atveju aš net nežinau, kas man pakenkė.

Supratau. Ačiū jums tada už pateiktus atsakymus.

SANTRAUKA

„DIRBTINIO INTELEKTO NAUDOJIMO TEISĖSAUGOS INSTITUCIJŲ VEIKLOJE IŠŠŪKIAI ŽMOGAUS TEISIŲ POŽIŪRIU“

Pasirinkta magistro baigiamojo darbo tema yra aktuali tiek užsienio ir Lietuvos Respublikos teisėsaugos institucijoms, kuriose naudojamos dirbtinio intelekto (DI) pagrindu veikiančios sistemos bei technologijos. Pritaikant DI sistemas bei technologijas renkami ir naudojami dideli kiekiai asmens duomenų, kas neužtikrinant atitinkamų saugiklių ir priežiūros pasaulio mastu kelia iššūkius asmens teisėms į privatumą ir duomenų apsaugą. Sugriežtintos duomenų apsaugos ir privatumo taisyklės ne tik pradėjo naują duomenų apsaugos reguliavimo etapą ES, bet kartu tapo pavyzdžiu bei atspirties tašku ir kitiems įstatymų leidėjams bei technologijų kūrėjams visame pasaulyje. DI ir technologijos leidžia daug tiksliau numatyti galimus nusikaltimus viešose vietose, taip pat gali padėti išaiškinti kitus nusikaltimus.

Teisėsaugos institucijos tiek kaip DI vartotojos, tiek kaip visuomenės saugumą užtikrinantys subjektai privalo imtis reikiamų priemonių, kad asmens teisės bei laisvės ir duomenų apsauga būtų maksimaliai užtikrintos. **Darbo objektas —** DI pagrindu veikiančių sistemų teisėsaugos institucijose taikymas žmogaus teisų požiūriu.

Darbo tikslas — atskleisti kilusius žmogaus teisių požiūriu iššūkius naudojant DI pagrindu veikiančias sistemas teisėsaugos institucijose.

Darbo uždaviniai:

1. Išnagrinėti DI sistemų bei technologijų istorinę raidą, DI sistemų tobulėjimą bei numatomą raidos strategiją;
2. Išanalizuoti, kokios galimos grėsmės kyla taikant DI pagrindu veikiančias sistemas bei technologijas teisėsaugos institucijose žmogaus teisių požiūriu;
3. Išnagrinėti DI pagrindu veikiančių sistemų bei technologijų praktinį taikymą teisėsaugos institucijose žmogaus teisių apsaugos kontekste.

Taikant DI pagrindu veikiančias sistemas bei technologijas teisėsaugos institucijose turi būti atkreipiamas dėmesys į LR Konstitucijoje numatytas asmens teises. Pagrindinė problema, kuri gali pažeisti žmogaus teisės ar laisvės pažeidimas, taikant DI pagrindu veikiančias sistemas bei technologijas. Ši iškilusi problema yra sprendžiama pasauliniu mastu. Aktyviai analizuojama ES lygmeniu, kuriame sprendžiama DI teisinė padėtis, bei bandoma numatyti DI ateitį, kad kuo mažiau būti pažeidžiama numatytu teisių ir laisvių.

SUMMARY

„CHALLENGES FROM THE PERSPECTIVE OF HUMAN RIGHTS IN THE ACTIVITIES OF LAW ENFORCEMENT OF ARTIFICIAL INTELLIGENCE "

The chosen topic of the master's thesis is relevant to both foreign and law enforcement institutions of the Republic of Lithuania, which use systems and technologies based on artificial intelligence AI. The application of AI systems and technologies involves the collection and use of large amounts of personal data, which poses challenges to individual rights to privacy and data protection without adequate safeguards and oversight worldwide. Tighter data protection and privacy rules have not only ushered in a new phase of data protection regulation in the EU, but have also set an example and a starting point for other legislators and technology developers around the world. DI and technology make it possible to predict potential crimes in public places much more accurately, and can also help detect other crimes.

Law enforcement authorities, both as users of AI and as actors in public security, must take the necessary measures to ensure that individual rights and freedoms and data protection are maximized. The aim of the work is to reveal the human rights challenges of AI - based systems in law enforcement. The object of the work is the application of AI - based systems in law enforcement institutions from the point of view of human rights.

Research tasks:

1. 1. To examine the historical development of AI systems and technologies, the improvement of IoT systems and the expected strategy;

2. To analyze the possible threats to the application of AI systems and technologies in law enforcement institutions from the point of view of human rights;

3. To examine the practical application of AI systems and technologies in law enforcement institutions in the context of human rights protection.

When applying the systems and technologies operating on the basis of AI in law enforcement institutions, attention must be paid to the rights of the person provided for in the Constitution of the Republic of Lithuania. The main problem that can violate human rights or freedoms through the use of AI systems and technologies. This problem is being addressed globally. There is an active analysis at EU level of the legal situation of AI, and an attempt to anticipate the future of AI in order to minimize violations of the rights and freedoms provided for.