

TEISĖ Į PRIVATUMĄ, ASMENS DUOMENŲ APSAUGĄ IR DIRBTINIS INTELEKTAS: TEISINIO REGULIAVIMO IŠŠŪKIAI LIETUVOJE IR EUROPOJE

Eglė Kavoliūnaitė-Ragauskienė



LSMC Teisės instituto mokslo tyrimai

Teisė į privatumą, asmens duomenų apsauga ir dirbtinis intelektas: teisinio reguliavimo iššūkiai Lietuvoje ir Europoje

Mokslo studija

Eglė Kavoliūnaitė-Ragauskienė



Lietuvos socialinių mokslų centro Teisės institutas,
Vilnius, 2023

Autorė

Dr. Eglė KAVOLIŪNAITĖ-RAGAUSKIENĖ, Lietuvos socialinių mokslų centro Teisés institutas

Recenzentai:

Prof. dr. Paulius Pakutinskas (Mykolo Romerio universiteto Teisés mokykla)

Prof. dr. Ramūnas Birštonas (Vilniaus universiteto Teisés fakultetas)

Kalbos redaktorė Dalia Gedzevičienė

Maketuotojas Rimantas Junevičius

Viršelio autorė Goda Dainauskaitė

Leidinj apsvarstė ir rekomendavo išleisti Lietuvos socialinių mokslų centro Teisés instituto Moksliinių leidinių aprobabimo komisija (2023 m. vasario 3 d., Nr. AP-2)

ISBN 978-609-8324-06-8

Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).



© Eglė Kavoliūnaitė-Ragauskienė, 2023
© Lietuvos socialinių mokslų centro Teisés institutas, 2023

TURINYS

JŽANGA	6
1. DIRBTINIO INTELEKTO SAMPRATA IR NAUDojimas VISUOMENĖS GYVENIME.....	10
1.1. Kaip atsirado dirbtinis intelektas?.....	11
1.2. Dirbtinio intelekto samprata ir rūšys	13
1.3. Dirbtinio intelekto naudojimo plėtra	18
1.4. Dirbtinio intelekto technologiniai sprendimai	21
1.5. Dirbtinio intelekto naudojimas privačiame ir viešajame sektoriuose.....	24
2. DIRBTINIO INTELEKTO NAUDojIMO KELIAMOS GRĒSMĖS VISUOMENEI IR INDIVIDAMS.....	31
2.1. Diskriminacija ir šališkumas.....	33
2.2. Susirinkimų laisvės galimi suvaržymai ir masinio sekimo grēsmės	34
2.3. Demografinis taikymas ir profiliaivimas.....	35
2.4. Manipuliacijų rizikos	36
2.5. Sprendimų nepaaiškinamumas	37
2.6. Asmens orumo pažeidimo rizika.....	38
2.7. Proporcingumo principo pažeidimai.....	39
2.8. Techninės ir saugumo rizikos	39
3. PRIVATUMO IR ASMENS DUOMENŲ SAMPRATA DIRBTINIO INTELEKTO KONTEKSTE	41
3.1. Privatumo ir asmens duomenų samprata ir teisinis reguliacijos Europos Sajungoje	41
3.2. Privatumo ir asmens duomenų apsaugos reguliacijos ir praktika Lietuvoje	47
4. DIRBTINIO INTELEKTO NAUDojIMO KELIAMOS GRĒSMĖS PRIVATUMUI.....	59
4.1. Dirbtinio intelekto pagalba rengant asmens duomenis.....	59
4.2. Veido atpažinimo sistemos naudojimas	62
4.3. Asmens duomenų sujungimas ir agregavimas.....	63

4.4. Sprendimų priėmimo pagrįstumas.....	66
4.5. Dirbtinio intelekto keliamos grėsmės privatumui praktikoje: Habitoskopinių duomenų registro Lietuvoje atvejis.....	67
5. DIRBTINIO INTELEKTO TEISINIO REGULIAVIMO PERSPEKTYVOS.....	71
 IŠVADOS.....	78
 LITERATŪRA	81
SUMMARY.....	89

Santrauka

Mokslo studijoje analizuojamos dirbtinio intelekto kūrimo ir naudojimo tendencijos, dirbtinio intelekto sistemų klasifikacijos ir jų poveikis žmogaus teisėms. Remiantis teisės aktais ir nacionalinių, Europos valstybių teismų bei Europos Žmogaus Teisių Teismo praktikos suformuluotais teisės į privatumą ir asmens duomenų apsaugą kriterijais vertinamos dirbtinio intelekto sistemų tendencijos ir bruožai, kurie kelia didžiausią grėsmę minėtomis žmogaus teisėms. Studijoje taip pat apžvelgiami Europos Sąjungos teisėkūros planai reguliuoti dirbtinio intelekto sistemas ir vertinamas jų pakankamumas tinkamai užtikrinti teisę į privatumą ir asmens duomenų apsaugą.

Pagrindiniai žodžiai: *dirbtinis intelektas, teisė į privatumą, duomenų apsauga, mašininis mokymasis.*

Dirbtinis intelektas visuomenės gyvenime – tiek teisėsaugos darbe, tiek privačiose iniciatyvose – naudojamas vis dažniau ir vis įvairesnėse srityse – užtikrinant visuomenės saugumą, vykdant eismo priežiūrą, renkant duomenis įvairiomis viešojo sektorius ataskaitoms, rinkodaros tikslais, pažinčių portaluose ir t. t. Dirbtinis intelektas jau yra tapęs svarbia mūsų gyvenimo dalimi. Kaip nurodoma viename pirmųjų Europos Sąjungos dokumentu, kalbančiu apie dirbtinį intelektą¹ – tai nebe mokslinė fantastika, o tikrovė, pradedant virtualiu asmeniniu asistentu organizuojant darbo dieną, baigiant keliavimui savarankiškai vairuojančia transporto priemone ir telefonais, siūlančiais dainas ar restoranus, kurie mums gali patikti. Dirbtinis intelektas ne tik palengvina mūsų gyvenimą, bet ir padeda išspręsti kai kuriuos didžiausius pasaulio iššūkius: nuo lėtinė ligų gydymo ar eismo įvykių mirtingumo mažinimo, kadangi apie 90 proc. eismo įvykių keliuose įvyksta dėl žmogiškos klaidos², iki kovos su klimato kaita ar kibernetinio saugumo grėsmių numatymo³. Pavyzdžiui, įvairose pasaulio šalyse naudojama „Clearview“ veido atpažinimo technologija, sukurta pasitelkiant „Facebook“ ir „Instagram“ svetainėse laisvai prieinamas nuotraukas, leidžia atpažinti asmenis. Greitai plėtojama bei tobulinama ir plačiai pritaikoma dirbtinio intelektu technologija renkami ir naudojami dideli kiekiai asmens duomenų, o tai, neužtikrinant atitinkamų saugiklių ir priežiūros tiek nacionaliniu, tiek Europos mastu, kelia iššūkių asmens teisei į privatumą ir duomenų apsaugą, ypač atsižvelgiant į tai, kad 90 % viso pasaulio duomenų buvo surinkti per pastaruosius penkerius metus.

Tokia situacija patraukė teisės į privatumą ir asmens duomenų apsaugos institucijų dėmesį visame pasaulyje, taip pat privertė reaguoti ir įstatymų leidėjus. Tačiau Europos Sąjungos pirminis tikslas yra lyderiauti pasaulyje kuriant ir naudojant dirbtinį intelektą įvairiuose viešojo ir privataus gyvenimo procesuose. Iš Europos Sąjungos lygmeniu priimtu programinių dokumentų aiškiai matyti, kad Europos Sąjunga

¹ Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui *Dirbtinis intelektas Europai*. COM/2018/237 final.

² Commission's report on Saving Lives: Boosting Car Safety in the EU. COM(2016) 0787 final.

³ Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui *Dirbtinis intelektas Europai*. COM/2018/237 final, p. 2

ketina konkuruoti su kitais pasaulio regionais plėtojant ir naudojant dirbtinio intelektu sistemas ir tam deda dideles intelektualines, ekonomines ir strategines pastangas.

Iki šiol dirbtinio intelekto sistemos, jų kūrimo ir naudojimo veikla gana nedaug specifiškai reguliuojami tiek Lietuvoje, tiek Europos Sąjungoje. Tiesa, dirbtinio intelekto kūrėjams ir naudotojams taikomi bendrieji Europos teisės aktai dėl pagrindinių teisių (pvz., duomenų apsaugos, privatumo, nediskriminavimo), vartotojų apsaugos, gaminių saugos ir atsakomybės. Šie principai turėtų būti taikomi bet kada – neprilausomai nuo to, kad paslaugą teikia ar funkciją vykdo dirbtinis intelektas, ar ne. Tačiau dėl tam tikrų dirbtinio intelekto ypatumų (pvz., nuolatinės technologinės pažangos gerinant duomenų kokybę, gebėjimo rinkti asmens duomenis vis iš įvairesnių šalių, sprendimų priėmimo nepaaiškinamumo ir kt.) šiuos teisės aktus gali būti sunkiau taikyti ir užtikrinti jų vykdymą. Taigi, buvo pripažinta, kad tam, jog būtų tinkamai apsaugotos žmogaus teisės, esamų teisinių instrumentų nepakanka, ir 2021 metais Europos Komisija pateikė Pasiūlymą dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas)⁴.

Labai greita dirbtinio intelekto kūrimo ir naudojimo plėtra verčia susirūpinti tinkamu žmogaus teisių, iškaitant asmens privatumo apsaugą ir duomenų apsaugą, užtikrinimu. Greita ir ypač nereguliuojama dirbtinio intelekto plėtra kelia įvairių iššūkių asmens privatumui, iškaitant asmens psichinę neliečiamybę, nediskriminavimui, nešališkumui, kyla grėsmė, kad gali būti suvaržytos susirinkimų ir saviraiškos laisvės, atsiranda nuogastavimų dėl galimo masinio asmenų sekimo, o tai kelia grėsmę demokratijai, taip pat dirbtinio intelekto naudojimas gali sudaryti sąlygas manipuliuoti asmenimis, ypač pažeidžiamais asmenimis, primygintai siūlant jiems pirkti tam tikras prekes ar paslaugas ar keisti savo politines, religines pažiūras arba įsitikinimus, taip pat asmenys patiria žalą dėl pasitelkus dirbtinį intelektą priimtų sprendimų, kurių argumentacijos neįmanoma atskleisti ir dėl to juos užginčtyi tampa labai sudėtinga.

Tačiau suvokiant poreikį reguliuoti dirbtinio intelekto plėtojimo ir naudojimo taisykles, Europos lygmeniu pabrėžiama, kad teisiniai ribojimai neturėtų užkirsti kelio dirbtinio intelekto plėtrai ar jos riboti, o turėtų nustatyti taisykles, kaip tai atlikti nekeiliant grėsmės žmogaus teisėms. Vis dėlto, kaip bus matyti iš šioje studijoje pateiktos analizės, kai kuriais atvejais tai padaryti yra labai sudėtinga ir tenka ieškoti kompromisų. Taip pat pažymėtina, kad dirbtinio intelekto kūrimo ir naudojimo plėtros tempas apsunkina tikslią ir aiškių teisės aktų, reguliuojančių dirbtinio intelekto kūrimą, pateikimą naudojimui ir taikymo nustatymą, kadangi labai greitai iškyla naujų situa-

⁴ Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai. COM(2021) 206 final.

ciųj, kai siūlomas reguliavimas tampa pasenęs arba nepakankamas. Atsižvelgiant į tai, siūlymai dėl dirbtinio intelekto reguliavimo yra lankstūs, aptakūs, su daug išimčių o tai irgi kelia grėsmę, kad praktikoje tai bus interpretuojama ne žmogaus teisių apsaugos naudai.

Mokslo studijos tikslas – atsižvelgiant į dirbtinio intelekto panaudojimo apimtis ir jų plėtrą, atskleisti Lietuvos ir Europos Sąjungos teisinio reguliavimo dėl dirbtinio intelekto naudojimo įvairiose srityse iššūkius, susijusius su grėsmėmis teisei į privatumą ir duomenų apsaugą, bei aptarti tobulintinas teisinio reguliavimo sritis.

Teisė į privatumą dirbtinio intelekto naudojimo kontekste Lietuvoje yra analizuota gana nedaug. Daugiausia publikuojami moksliniai komentarai apie bendrąsias grėsmes privatumui (pvz., Jurčys, P. *Asmeninių duomenų nuosavybė*⁵; Kalpokas, I. *Dirbtinio intelekto poveikis žmogaus teisėms nėra išimtis*⁶ ir kt.). Dirbtinio intelekto naudojimą visuotiniam sekimui, akcentuojant grėsmę asmens privatumui, nemažai analizavo P. Griciūnas (pvz., žr. Griciūnas, P. *Už jūsų ir mūsų laisvę*⁷; Griciūnas, P. *Pasikinkius „Pegasą“: elektroninių sekimo priemonių mitai ir tikrovė*⁸). Užsienyje ši tema analiuota kur kas plačiau, tiriami įvairūs dirbtinio intelekto iššūkiai privatumui (pvz., žr. Stahl, B. C., Wright, D. *Ethics and privacy in AI and big data: Implementing responsible research and innovation*⁹; Rodrigues, R. *Legal and human rights issues of AI: Gaps, challenges and vulnerabilities*¹⁰; Humerick, M. *Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence*¹¹; Mantelero, A. *AI and Big Data: A blueprint for a human rights, social and ethical impact assessment*, kt.).

Nemažai ši tema tyrinėta ir rengiant ES teisės aktus, kuriais siekiama suderinti dirbtinio intelekto naudojimą ES (pvz., Europos Komisijos baltoji knyga „Dirbtinis

⁵ Jurčys, P. Asmeninių duomenų nuosavybė. *Teisė.Pro*, 2020-08-01. Prieiga per internetą: <https://www.teise.pro/index.php/2020/08/11/p-jurcys-asmeniniu-duomenu-nuosavybe/>.

⁶ Kalpokas, I. Dirbtinio intelekto poveikis žmogaus teisėms nėra išimtis. *VDU.lt*, 2021-12-01. Prieiga per internetą: <https://www.vdu.lt/litdirbtinio-intelekto-poveikis-zmogaus-teisems-nera-isimtis/>.

⁷ Griciūnas, P. Už jūsų ir mūsų laisvę. *IQLIFE*, 2021-01-13. Prieiga per internetą: <https://zurnalas.iqlife.lt/advokatas/pries-jusu-ir-musu-laisve/216478>.

⁸ Griciūnas, P. Pasikinkius „Pegasą“: elektroninių sekimo priemonių mitai ir tikrovė. *IQLIFE*, 2022-01-18. Prieiga per internetą: <https://zurnalas.iqlife.lt/advokatas/pasikinkius-pegasa-elektroniniu-sekimo-priemoniu-mitai-ir-tikrove/243188>.

⁹ Stahl, B. C., Wright, D. Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, 2018, Vol. 16, Issue 3.

¹⁰ Rodrigues, R. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 2020, Vol. 4.

¹¹ Humerick, M. Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence. *Santa Clara High Tech. LJ*, 2018, Vol. 34, Issue 4, p. 393.

intelektas. Europos požiūris į kompetenciją ir pasitikėjimą¹²; Europos Komisijos Patikimo dirbtinio intelekto gairės¹³; Komisijos komunikatas „Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas“¹⁴ ir kt.).

Studiją sudaro penkios pagrindinės dalys. Pirmojoje analizuojamos dirbtinio intelekto sistemos – aptariama dirbtinio intelekto samprata, raidos istorija, plėtojimo perspektyvos, pristatomos dirbtinio intelekto rūšys ir atsižvelgiant į jų skirtumus preliminariai įvertinamas galimas poveikis žmogaus teisėms. Antrojoje studijos dalyje aptariamos su dirbtinio intelekto naudojimu susijusios rizikos ir grėsmės individualiams asmenims ir visuomenei, t. y. aptariami veiksnių, paskatinę imtis reguliacinių dirbtinio intelekto iniciatyvų. Trečiojoje dalyje analizuojamos Europos Sąjungos, Europos valstybių ir Lietuvos teisės į privatumą ir asmens duomenų apsaugą užtikrinimo nuostatos, kurios yra reikšmingos vertinant, ar dirbtinio intelekto kūrimo ir naujodimo praktika nepažeidžia šių teisių. Ketvirtoji studijos dalis skirta išsamiai analizuoti dirbtinio intelekto kūrimo ir naudojimo plėtros aspektus, kurie kelia grėsmę asmens privatumui ir duomenų apsaugai ir kuriems turėtų būti skiriamas ypatingas reguliacinis dėmesys. Galiausiai penkojoje studijos dalyje tiriami dirbtinio intelekto teisinio reguliavimo planai ir perspektyvos, įvertinant, ar ir kiek jie padės užtikrinti teisę į privatumą ir asmens duomenų apsaugą atsižvelgiant į ankstesnėje dalyje išskirtas grėsmes.

¹² Europos Komisija. Baltoji knyga. *Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą*. COM(2020) 65 final.

¹³ Europos Komisija. *Patikimo dirbtinio intelekto gairės*. Prieiga per internetą: <https://op.europa.eu/lt-publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.

¹⁴ Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. *Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas*. COM(2019) 168 final.

1. DIRBTINIO INTELEKTO SAMPRATA IR NAUDOJIMAS VISUOMENĖS GYVENIME

Pastaraisiais metais dirbtinis intelektas buvo viena svarbiausių viešojo ir privataus sektorių temų ir tikėtina, kad artimiausiais metais dėmesys jai nemažės. Jau yra pasiektais lygmuo, kad dirbtinis intelektas gali galvoti, daryti išvadas ir priimti sprendimus kaip protinges žmogus. Kaip bus apibūdinta vėliau, kai kuriose srityse dirbtinio intelekto gebėjimai jau lenkia žmones. Tačiau šiuo metu plačiausiai dirbtinis intelektas naudojamas užduotims, susijusiomis su modelių atpažinimu, išvadų darymu, sprendimų priemimu kiekvienu konkrečiu atveju arba įsitraukimu į pokalbij, vykdyti. Dažniausiai dirbtinio intelekto savoka suprantama kaip bendras terminas, apimantis įvairias technologijas, kurių kiekviena skirta tam tikros rūšies problemai išspręsti. Dirbtinio intelekto naudojimas plečiasi eksponentiškai: nuolat didėja duomenų kiekių, iš kurio dirbtinio intelekto modeliai gali mokytis, taip pat didėja algoritmų ir platformų įvairovė, kurias ekosistemos, kuriose galima išbandyti ir įdiegti įvairius dirbtinio intelekto panaudojimo sprendimus¹⁵.

Dirbtinis intelektas naudojamas įvairiausiose srityse ir padeda žmonijai vykdyti daugybę veiklų. Pavyzdžiui, Danijoje dirbtinis intelektas padeda gelbėti gyvybes leidamas skubiosios pagalbos tarnyboms diagnozuoti širdies sustojimą ar kitas sąlygas pagal skambinančiojo balso garsą. Austrijoje jis padeda radiologams tiksliau aptikti navikus, realiu laiku lygindamas rentgeno nuotraukas su daugybe kitų medicininii duomenų. Daugelis ūkių visoje Europoje jau naudoja dirbtinį intelektą savo gyvūnų judėjimui, temperatūrai ir pašarų suvartojimui stebeti. Tada dirbtinio intelekto sistema gali automatiškai pritaikyti šildymo ir šerimo įrenginius, kad padėtų ūkininkams stebeti savo gyvūnų gerovę ir sudarytų galimybes vietoje to atliliki kitus darbus¹⁶.

¹⁵ European Commission/Deloitte. Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security. Volume 2: Addendum, p. 1. Prieiga per internetą: <https://op.europa.eu/en/publication-detail/-/publication/69f33ff7-a156-11ea-9d2d-01aa75ed71a1/language-en>.

¹⁶ Europos Komisija, 2018, p. 2.

1.1. Kaip atsirado dirbtinis intelektas?

Nors dirbtinis intelektas, atrodo, visai neseniai buvo pradėtas naudoti teikiant viešias ir privačias paslaugas, dirbtinio intelekto tyrimai ir bandymai taikyti praktikoje yra nenujas reiškinys – jo ištakos siekia 1950-uosius, kai filosofas matematikas Alanas Turingas savo moksliniame straipsnyje „Skaičiavimo mašinos ir intelektas“ (angl. *Computing Machinery and Intelligence*) svarstė klausimą apie tai, ar mašinos gali mąstyti. Atsižvelgdamas į tai, kad tiksliai apibrėžti žodį „mąstyti“ yra sudėtinga, jis pasiūlė tai aiškintis kitaip, naudojant trijų asmenų žaidimą, pavadinę „imitacinis žaidimas“ (angl. *imitation game*). Šio žaidimo tikslas – vienas žaidėjas („tyréjas“) turi išsiaiškinti, kuris iš kitų dalyvių yra kompiuteris, o kuris – žmogus, kai atsako į klausimus raštu, t. y. iškeltas klausimas, ar kompiuteris gali bendrauti taip natūraliai, kad apgautų žmogų, kuris pamanytų, kad kalbasi su tikru žmogumi? Turingas šią mintį perėmė iš žaidimo, kai asmuo, vadinas klausinėtoju, turi nustatyti, ar kitame kambaryje esantis atsakinėtojas yra vyras ar moteris. Savo teoriniame eksperimente jis atsakinėtoją pakeitė kompiuteriu. Dabar tai vadinama Turingo testu, kuriam atliki kompiuteris privalo atsakinėti taip lingvistiskai išmoningai, kaip tai daro žmogus. Kiek vėliau, 1956-aisiais, sėvoka „dirbtinis intelektas“ buvo vartojama Dartmuto koledže praktiniame seminare. Keli mokslininkai (Allen Newell, Herbert Simon, John McCarthy, Marvin Minsky ir Arthur Samuel) pradėjo tyrinėti dirbtinį intelektą – kartu su studentais kūrė programas, kurios gebėjo mokytis tikrinimo strategijų ir kurias spauda įvertino kaip „neįtikėtinas“. Šis įvykis žymi dirbtinio intelekto aukso amžiaus pradžią.

1997-aisiais „IBM Deep Blue“ – šachmatais žaidžiantis superkompiuteris – įveikė Garry Kasparovą šachmatų partijoje. Tai buvo pirmasis kartas, kai kompiuterinė sistema laimėjo prieš tuometinį pasaulio čempioną žaisdama pagal standartinį šachmatų žaidimo laiko skaičiavimą. „Deep Blue“ laimėjimas buvo laikomas simboline dirbtinio intelekto pergale, žyminčia lūžio tašką, kai kompiuterinė sistema įveikė geriausią planetos žaidėją. Nepaisant to, kad šachmatai yra strateginis žaidimas, tame yra palyginti nedaug pasirinkimų ir galimų išeicių kiekvienam žaidimo momente. Todėl tokiu būdu užprogramuoti kompiuterį nėra labai sudėtinga. Kai kompiuteris laimėjo šachmatų partiją prieš stipriausią planetos žaidėją, atejo laikas jį tobulinti toliau, ir tam buvo pasirinktas Kinijoje populiarus stalų žaidimas „Go“, kuriame yra kur kas daugiau galimybų pasirinkti įjimus. Todėl reikėjo gerai padirbėti, kol 2017 metais „Google DeepMind's“ sukurta „AlphaGo“ kompiuterinė programa nugalėjo „Go“ žaidimo pasaulio čempioną Ke Jie.

2017 metų pabaigoje „AlphaGo“ buvo patobulintas nauja versija „AlphaGo Zero“. Ši sistema neturėjo jokių duomenų apie žaidimą ir „mokėsi“ žaisdama prieš savo pag-

rindinę versiją, kuri turėjo įdiegtus „Go“ žaidimo éjimų algoritmus. Patobulinta „AlphaGo Zero“ versija „išmoko“ tiek, kad laiméjo prieš savo pagrindinę versiją, kuri turėjo įdiegtus algoritmus. Savo éjimų racionalumuji net aplenké savo pirmtakę versiją, kurią užprogramavo žmonės.

Dirbtinio intelekto raida gali būti apibendrinta taip:

- 1950 metai: Alano Turingo mokslinis darbas „Ar mašinos gali mąstyti“ pirmą kartą pateiké dirbtinio intelekto koncepciją.
- 1955 metai: Karnegio technologijų institute pademonstruota pirmoji dirbtinio intelekto programa „Logikos teoretikas“.
- 1956 metai: mokslininkas Johnas McCarthy apibréžė sąvoką „dirbtinis intelektas“, kalbédamas apie mokslą kuriant mąstančias mašinas.
- 1957 metai: Frankas Rosenblattas sukûré pirmajį dirbtinį neuronų tinklą.
- 1961 metai: UNIMATE, pirmasis „General Motors“ pramoninis robotas, pa-keitė žmones pramonés surinkimo linijoje.
- 1964 metai: ELIZA, MIT sukurtas pokalbių robotas (angl. *chatbot*), pradéjo pokalbius su žmonėmis.
- 1966 metai: pristatytas pirmasis mobilusis robotas „Shakey“, kuris gali stebéti ir priimti sprendimus remdamasis tuo, kas yra jo aplinkoje.
- 1967 metai: pradedamas kurti artimiausio kaimyno algoritmas¹⁷, nuo kurio pradétos plétoti kompiuteriu grindžiamos bruožų atpažinimo sistemos.
- 1979 metai: Stanfordo universiteto studentai sukûré savarankiškai naviguojan-či automobilių¹⁸.
- 1981 metai: Geral’as DeJong’as pristatė EBL (paaiškinimu grindžiamą moky- mąsi, angl. *explanation based learning*), kai kompiuteris galéjo sukurti taisyklių rinkinius remdamasis mokymosi duomenimis.
- Karnegio Melono universitetas sukûré „NavLab“, pirmą autonominšką automo- bilį. Panašiu metu tą atliko ir „Mercedes Benz“.
- 1997 metai: „Deep Blue“, IBM mašina, laiméjo šachmatų partiją prieš Garry Kasparovą, tuometinį pasaulio šachmatų čempioną.
- 1998 metai: MIT pristatė „KISmet“, emocionaliai protingą robotą, kuris atpa- žista žmogaus jausmus ir reaguoja į juos.
- 1999 metai: „Sony“ pradéjo prekiauti pirmu augintinio šuniuko robotu „AiBO“, kuris bégant laikui galéjo išsiugdyti tam tikrus įgūdžius.

¹⁷ Wikipedia. *Nearest neighbour algorithm*. Prieiga per internetą: https://en.wikipedia.org/wiki/Nearest_neighbour_algorithm.

¹⁸ Stanford’s robotics legacy. Prieiga per internetą: <https://news.stanford.edu/2019/01/16/stanfords-robotics-legacy/>.

- 2002 metai: sukurtas „Roomba“, pirmasis išmanusis vakuuminis „iRobot“ siurblys. Jis gali pats naviugoti ir valyti namus.
- 2006 metai: Geoffrey Hintonas pradėjo vartoti naują savoką „gilusis mokymasis“ (angl. *deep learning*) aiškindamas naujus algoritmus, kurie įgalina kompiuterius atskirti objektus, vaizdus ir vaizdo įrašus.
- 2010 metai: išleistas „Microsoft Kinect“, kuris stebi 20 žmogaus funkcijų, leidžiančių žmonėms bendrauti su kompiuteriu judesiais ir gestais.
- 2011 metai: „Apple“ įdiegė „Siri“ į „iPhone 4S“, dirbtiniu intelektu pagrįstą virtualų asistentą, kurį įgalina balso komandos. Taip pat šiais metais IBM mašina „Watson“ įveikė du didžiausius žaidimo „Jeopardy!“¹⁹ nugalėtojus.
- 2014 metai: „Amazon“ pristato „Alexa“, virtualų balso komandomis bendraujančią asistentą.
- 2015 metai: JAV specialiųjų operacijų vadovybė pristatė roboto egzoskeleto idėją, siekdama sustiprinti kario pojūčius.
- 2017 metai: „Google“ dirbtinis intelektas „AlphaGo“ nugalėjo žaidimo „Go“ pasaulio čempioną.
- 2018 metai: pradėtas tyrimas dėl dirbtinio intelekto, nes pranešama apie nesaugią ir prastą „IBM Watson“ ir „Amazon“ atpažinimo įrankio praktiką. Šiais metais įvyko dirbtinio intelektu plėtojimo ir naudojimo proveržis. Dirbtinis intelektas pradedamas naudoti daugelyje kasdienio gyvenimo sričių. „Tesla“ buvo viena iš pirmųjų automobilių gamintojų, pradėjusi gaminti savarankiskai važiuojančią transporto priemonę. Stengdamiesi neatsilikti nuo „Tesla“, daugelis tradicinių automobilių gamintojų užsibrėžia tikslą išleisti savo savarankiskai važiuojančius automobilius iki dešimtmečio pabaigos.
- 2019 metai: „Google AlphaStar“ nugalėjo „StarCraft 2“ žaidėjus. Dirbtinio intelekto agentas turėjo susidoroti su matomais priešais tuo pat metu turėdamas analizuoti įvairias žemėlapio sritis²⁰.

1.2. Dirbtinio intelekto samprata ir rūšys

Remiantis Europos Komisijos 2018 metais pateiktu apibrėžimu, dirbtinis intelektas – tai sistemos, kurios elgiasi protingai, analizuodamos savo aplinką ir darydamos gana savarankiskus sprendimus tikslui pasiekti. Šios intelekto sistemos gali būti grindžiamos vien tik programine įranga ir veikti virtualiajame pasaulyje (pvz., balso sin-

¹⁹ Wikipedia. *Jeopardy!* Prieiga per internetą: <https://en.wikipedia.org/wiki/Jeopardy!>.

²⁰ European Commission/Deloitte, 2018, p. 190–191.

tezatoriai, vaizdo analizės programinė įranga, paieškos sistemos, kalbos ir veido atpažinimo sistemos) arba gali būti integruotos techninėje įrangoje (pvz., pažangiuose robotuose, savaeigėse transporto priemonėse, bepiločiuose orlaiviuose ar daiktų interneto objektuose)²¹.

Dirbtinis intelektas yra bendriausias terminas, apibūdinantis mašiną, pasižymintą bet kokios rūšies protingu elgesiu. Dirbtinio intelekto mašinos yra programos, kurių jaučia, samprotauja, veikia ir prisitaiko taip, kaip gali daryti žmonės. Dirbtiniu intelektu laikomos įvairios technologijos (nors labiausiai paplitusi yra mašininis mokymasis (angl. *machine learning*, kaip apibūdinta toliau). Tačiau ne visos dirbtinio intelekto mašinos yra susijusios su mašininiu mokymusi, pavyzdžiui, „ekspertinė sistema“ (angl. *expert system*) yra kur kas paprastesnė dirbtinio intelekto sistema, kuri nesimoko iš duomenų, o susideda iš individualiai sukurtų taisykių, kurias dažniausiai specialistai suprogramuoja įrenginyje. Vienas iš tokų pavyzdžių yra „Stockfish“²² – žaidimo šachmatais algoritmas, kuris įvertina éjimo galimybes, remdamasis tiksliai atliku statistiniu vertinimu (priešingai nei mokymasis iš istorinių žaidimų).

Mašininis mokymasis (angl. *machine learning*) yra viena didžiausių ir žinomiausių dirbtinio intelekto rūsių. Jį sudaro skirtingi mokymo modelių algoritmai. Kitaip tariant, mašininis mokymasis leidžia sistemoms mokytis tiesiogiai iš duomenų, nustatyti modelius ir priimti sprendimus su minimaliu žmogaus įsikišimu. Pavyzdžiui, jei norime, kad algoritmas atpažintų el. pašte esantį šlamštą, galime pateikti el. laiškų, kurie rankiniu būdu pažymėti kaip šlamštas arba ne šlamštas, pavyzdžių. Algoritmas nustato šių mokymo duomenų šablonus ir naudoja juos, kad nuspėtų, ar naujas el. laiškas iš ne mokymo duomenų rinkinio yra šlamštas, ar ne.

Sudétingesnės sistemos – neuroniniai tinklai – yra algoritmai, sukurti pagal žmogaus smegenis, tačiau nėra jiems lygiaverčiai. Neuroniniai tinklai susideda iš apdorojimo mazgų, sujungtų tarpusavyje, kad sudarytų tinklą. Apdorojimo mazgai naudoja svorius duomenims transformuoti; siekiant sukurti prasmingus šios transformacijos rezultatus, svoriai turi atitikti tam tikras reikšmes. Norint sužinoti šias vertes, tinklas turi būti apmokytas naudojant optimizavimo metodus, o tai reiškia, kad neuroniniai tinklai gali būti laikomi mašininio mokymosi porūšiu²³.

Gilusis mokymasis reiškia neuroninių tinklų porūšį (taigi ir mašininį mokymąsi), paprastai naudojamą „pažinimo“ užduotims, tokioms kaip kalbos atpažinimas, vaiz-

²¹ Europos Komisija, 2018.

²² Stockfish 15. Prieiga per internetą: <https://stockfishchess.org/>.

²³ OECD Working Papers on Public Governance. Hello, World. Artificial intelligence and its use in the public sector. 2019, p. 56. Prieiga per internetą: <https://www.oecd-ilibrary.org/docserver/726fd39d-en.pdf?Expires=1666023983&id=id&accname=guest&checksum=2B0678AFDEB937C7A5B42575C7C96F44>; European Commission/Deloitte, p. 11.

dū atpažinimas ar kitokios prognozės, atliskti. Sąvoka „gilusis“ reiškia didelį sluoksnių skaičių; dideli neuroniniai tinklai turi didesnę nuspėjamąją galią, tačiau jiems reikia daugiau duomenų ir skaičiavimo (mažesni neuroniniai tinklai šiai laikais naudojami retai). Sluoksniai tarp neuroninio tinklo įvesties ir išvesties sluoksnių vadinami „pasléptais sluoksniais“. Kai tinklas yra treniruojamas, sluoksniai tampa jautrūs tam tikroms įvesties ypatybėms, o semantinis sudėtingumas didėja, kai tinklas auga²⁴.

Arthur'as Samuel'is, amerikiečių inžinierius ir kompiuterių mokslininkas, vienas iš dirbtinio intelekto plėtojimo pionierių, mašininį mokymąsi apibrėžia taip: „Mašininis mokymasis yra studijų sritis, suteikianti kompiuteriams galimybę mokytis bei aiškaus užprogramavimo.“ Šio apibrėžimo esmė yra paskutinė dalis („<...> be aiškaus užprogramavimo“), dėl kurios ji labai skiriasi nuo kitų metodų. Taikant tradicinius metodus, analitinė logika yra užkoduota aiškiai (paprastas pavyzdys būtų „jeigu A, tai B“, t. y. duodamos instrukcijos atliskti tam tikrą veiksmą, jei įvyksta koks nors įvykis). Priešingai, mašininio mokymosi modelis yra pagrįstas duomenimis; paprastai inicijuojama kaip tam tikra modelio architektūra su tikslu (pvz., sumažinti regresijos paklaidą), modelio architektūros parametrai koreguojami taip, kad modelis būtų optimizuotas savo tikslui (t. y. „mokytais“). Tai sukuria labai skirtinę paradigmą lyginant su tradicinėmis analitinėmis sistemomis, kuriose modeliai yra „mokomi“ ir „testuojami“, o tam, kad sistemos būtų produktyvios, reikia daug duomenų ir didelės skaičiavimo galios. Mašininis mokymasis taip pat skirstomas į prižiūrimą mokymąsi (angl. *supervised learning*), neprižiūrimą mokymąsi (angl. *unsupervised learning*) ir skatinamąjį mokymąsi (angl. *reinforcement learning*).

Prižiūrimo mokymosi atveju mokymo duomenys yra pažymėti „teisingu atsakymu“ kiekvienam pavyzdžiui. Pavyzdžiui, klasifikuojant, ar vaizdas yra šuo ar katė, algoritmas sužinos, kas yra katė ir šuo, analizuodamas jam pateiktas mokymosi taisykles. Šiuo atveju modelio pateiktas rezultatas visada bus tik „šuo“ arba „katė“.

Mokymasis be priežiūros yra tuo atveju, kai mokymo duomenų rinkinyje nėra jokių žymėtų duomenų. Aukščiau pateikto „kačių ir šunų“ pavyzdžio atveju taisyklių rinkinyje būtų vaizdai, bet be etikečių, kuris gyvūnas pavaizduotas. Neprižiūrimas mokymasis bando nustatyti ryšius, panašumus ir skirtumus, esančius šiuose nepažymėtuose duomenyse, ir juos sugrupuoti.

Skatinamasis mokymasis įgalina mašiną mokytis naudojant atlygi ir bausmes formulujant agentais pagrįstas problemas. Agentu pagrįsta problema yra ta, kai mašina gali atliskti veiksmus tam tikroje aplinkoje, priklausomai nuo to, kaip problema suformuluota. Laikui bėgant aparatas išmoksta maksimaliai padidinti savo atlygi ir užtik-

²⁴ European Commission/Deloitte, p. 11.

rina rezultatus, skatinamus kaupiant atlygi (pavyzdys galėtų būti transporto priemonė, siekiant maksimaliai išnaudoti savo laiką kelyje ir išvengti susidūrimų ar bausmių). Mokslininkai iš „Salesforce“, žinomas debesų kompiuterijos įmonės, naudojo skatinamąjį mokymąsi kartu su pažangiu kontekstinio teksto generavimo modeliu, kad sukurtų sistemą, galinčią sudaryti labai ilgų tekstų santraukas. Anot jų, algoritmas gali būti apmokytas naudojant įvairių tipų medžiagą (naujienų straipsnius, tinklaraščius ir kt.).

Egzistuoja ir daugiau dirbtinio intelekto sistemų klasifikacijų. Pavyzdžiui, američių mokslininkas Thomas H. Davenport'as pateikė dirbtinio intelekto klasifikaciją pagal jo naudojimo paskirtį, o ne naudojamas technologijas. Jis išskiria:

Dirbtinio intelekto automatizavimas – galima naudoti dirbtinį intelektą, siekiant palengvinti sudėtingų vidinių procesų automatizavimą. Tokia veikla skiriasi nuo paprastesnio automatizavimo, nes reikia didesnio intelekto, pavyzdžiui, prisiaikymo. Tarkime, tai galėtų būti neapmokėtų sąskaitų aptikimas el. pašte ir tokų sąskaitų surūšiavimas.

Dirbtinio intelekto įžvalgos – tai atvejai, kai dirbtinis intelektas ne tik aptinka duomenis, bet ir analizuja juos, kad pateiktų ateities prognozes ar rekomendacijas. Paiteikus sistemai naujų duomenų, prognozės laikui bėgant gali tapti tikslėnės.

Dirbtinio intelekto įsitraukimas – t. y. dirbtinio intelekto naudojimas siekiant sukurti automatinį duomenimis pagrįstą personalizavimą. Šiam dirbtinio intelekto tipui paprastai reikia dviejų ankstesnių dirbtinio intelekto savybių (automatizavimo ir įžvalgų). Šio tipo dirbtinio intelekto pavyzdys galėtų būti pokalbių robotai²⁵.

Dirbtinio intelekto sistemos gali būti klasifikuojamos ir pagal raidos etapą. Atsižvelgiant į tai, kad dirbtinio intelekto terminas vartoamas tiek siekiant apibūdinti sudėtingus procesus, kur dirbtinio intelekto įžvalgos viršija žmogaus gebėjimus, ir visai paprastus sprendinius, kurie tik padeda žmonėms atliki rutininius veiksmus, teoriuje išskiriama dirbtinio intelekto sistemų skirtumai pagal jų raidą.

Siaurasis dirbtinis intelektas (angl. *Artificial Narrow Intelligence* arba *ANI*), dar vadinamas silpnuoju dirbtiniu intelektu – tai sistemos, kurios specializuojasi vienoje srityje ir yra skirtos labai specifinėms užduotims atliki, pavyzdžiui, aptikti konkretius objektus vaizduose arba valdyti konkrečias mašinas. Siaurojo dirbtinio intelekto sistemos įgyvendina statistinius modelius ir greitai tampa nebeaktualios, kai modelis pasikeičia nuo tos versijos, kai buvo sukurtos taisyklės dirbtiniams intelektui taikyti. Pavyzdžiui, pokalbio padėjėjai, esantys išmaniuosiuose telefonuose, gali bendrauti panašiai kaip žmogus, tačiau dažniausiai apsiriboją siauromis galimų komandų ir dia-

²⁵ European Commission/Deloitte, p. 12.

logo sritimis. Iki šiol mobiliosiuose telefonuose yra naudojamos tik siaurojo dirbtinio intelekto sistemos. Analogiškai siaurojo dirbtinio intelekto pavyzdys gali būti veido atpažinimas ir savarankiškai važiuojantys automobiliai. Šios sistemos sutelkia dėmesį į vieną konkrečią užduotį su aiškiais apribojimais. Moksliniai tyrimai vis dar vyksta siekiant sukurti platesnes sistemas.

Bendrasis dirbtinis intelektas (angl. *Artificial General Intelligence* arba *AGI*), dar vadinamas stipriuoju dirbtiniu intelektu – tai sistemos, galinčios atlirkti daugybę užduočių, kurioms paprastai prireiktų žmogaus įsikišimo. Vienas iš tokų sistemų pavyzdžiu galėtų būti dirbtinis intelektas, valdantis robotą, gebantį spręsti naujas motorines užduotis, su kuriomis susiduria fizinėje aplinkoje. Sėkmingai sprendžiant viena kitą papildančias, bet skirtingas problemas, galima tikėtis, kad bendrojo dirbtinio intelekto sistemos atskleis gebėjimą planuoti elgesį (parinkti tam tikrą veiksmų seką ir trukmę atsižvelgiant į reiškinio tendencijas) ilgalaikėje perspektyvoje.

Dirbtinis superintelektas (angl. *Artificial Super Intelligence* arba *ASI*) – tai sistemos, kurios gerokai pranoktų žmones atliekant pažinimo reikalaujančias užduotis virose srityse, iškaitant mokslinį kūrybiškumą ir socialinius įgūdžius. Tai kol kas yra hipotetinė koncepcija ir ekstrapoliacijos rezultatas, kuriuos bendrojo dirbtinio intelekto sistemos, turinčios prieigą prie didžiulio duomenų kiekiei ir skaičiavimo galios, turi galimybę pasiekti.

Kaip jau buvo minėta, šiuo metu plačiai naudojamos tik siaurojo dirbtinio intelekto sistemos, tokios, kaip veido atpažinimas ir savarankiškai važiuojantys automobiliai. Šios sistemos sutelkia dėmesį į vieną konkrečią užduotį su aiškiais apribojimais²⁶.

Atkreiptinas dėmesys, kad nors ankstesniuose dirbtinio intelekto raidos etapuose dirbtinis intelektas galėjo būti suprantamas ir kaip procesų automatizavimas, dabar jau daromas skirtumas tarp šių sąvokų. Automatizavimas reiškia iš anksto užprogramuotas taisykles, kurios turi vieną tikslą – atlirkti pasikartojančias užduotis ir pakeisti žmogaus darbą. Tokios programos yra statinės, nekintančios ir susietos su tam tikrais kodais. Automatizuotos sistemos laikui bégant nesikeičia ir yra valdomos rankiniu konfigūravimu. Automatizavimas padeda įmonėms, nes darbuotojai, užuot vykdę nuolat besikartojančias užduotis, gali sutelkti dėmesį į sudėtingesnį ir kūrybiškesnį darbą. Pavyzdžiui, jei reikia atspausdinti kelis vienodus pranešimus, galima užprogramuoti kompiuterį, kad jis visus pranešimus spausdintų kartu, užuot spausdinęs kiek-vieną pranešimą atskirai. Be to, dirbtinis intelektas atkartoja žmogaus mąstymą. Dirbtinio intelekto programoms dažnai reikia didelio duomenų kiekiei, iš kurio jos „mokosi“ ir pasiekia tam tikrus rezultatus. Skirtingai nei automatizavimas, dirbtinis inte-

²⁶ European Commission/Deloitte, p. 189.

lektas skirtas nuolat ieškoti modelių ir tendencijų, mokytis iš patirties ir panašiose situacijose pateikti panašius atsakymus. Tačiau visada išlieka pavojus, kad dirbtinis intelektas padarys klaidą, jei neteisingai interpretuos duomenis ar neteisingai juos priskirs tam tikrai kategorijai²⁷.

1.3. Dirbtinio intelekto naudojimo plėtra

Akivaizdu, kad pasaulio lygiu technologijos evoliucionuoja beprecedenčiu greičiu. Pagrindiniu valstybių ekonomikos ir politikos, net ir socialinio gyvenimo varikliu tapo nebe gamyba, o duomenys. Kai kas duomenis netgi pradėjo vadinti „naujaja nafta“. Didėja „didžiųjų duomenų“ (angl. *big data*) apimtys, o dirbtinis intelektas vis daugiau ir tiksliau iš šio duomenų srauto geba sugeneruoti naudingų ižvalgų, kokių paprastas žmogus savo mąstymo ribose negalėtų padaryti. Atvirkščiai, kuo daugiau duomenų yra atveriamos, tuo daugiau ir įvairesnių tendencijų ir taisyklių gali numatyti ar sukurti dirbtinis intelektas. Jis grindžiamas technologinėmis galimybėmis „mokyties“ iš duomenų, ir tai sudaro galimybes tam tikrų problemų ar situacijų sprendimą perkelti iš žmonių į kompiuterines sistemas. Be to, dirbtinis intelektas gali ne tik atliliki retrospektyvią analizę, jis gali prognozuoti tam tikrus įvykius ir tendencijas remdamasis istoriniais duomenimis apie procesų eigą. Prognozuojama, kad naudojant dirbtinį intelektą padidės įvairių sričių produktyvumas, kadangi dirbtinis intelektas gali paskatinti reikšmingus patobulinimus įvairose pramonės šakose. Tik ribotas išradimų skaičius žmonijos istorijoje (įskaitant garo variklius ir internetą) turėjo tikrai platų poveikį, paskatino naujoves ir stipriai paveikė ekonomiką bei visuomenę. Tikimasi, kad dirbtinis intelektas pagerins esamus produktus ir paslaugas, sukurs viškai naujų, optimizuos vidines verslo operacijas automatizuodamas ir palaikydamas sprendimus bei sukurs naujų galimybų naudoti ir tobulinti patį dirbtinį intelektą²⁸.

Atsižvelgdamos į sparčią dirbtinio intelekto raidą ir jo panaudojimo plėtrą, daugelis valstybių paskelbė nacionalines dirbtinio intelekto strategijas ar sistemas, skirtas augimui skatinti, ir šiuos siekius remia investicijomis, programomis ir partneryste. Lietuva taip pat yra patvirtinusi Dirbtinio intelekto strategiją²⁹, kurios tikslas – remiantis esamais ištekliais, patirtimi ir potencialu, tapti regiono lydere, padidinti Lietuvos konkurencingumą tarp Europos Sąjungos šalių ir sėkmingai išitraukti į pasau-

²⁷ European Commission/Deloitte, p. 11–12.

²⁸ European Commission/Deloitte, p. 9.

²⁹ Lietuvos Respublikos ekonomikos ir inovacijų ministerija. Kurk Lietuvai. *Lietuvos dirbtinio intelekto strategija*. Prieiga per internetą: [https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT\(1\).pdf](https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf).

linę dirbtinio intelekto ekosistemą. Šioje strategijoje pateikiamos rekomendacijos, kaip padidinti dirbtinio intelekto sistemų naudojimą viešajame ir privačiame sektoriuose (pvz., privačiame sektoriuje skatinti įmones, savo sektoriaus pirmtakes, diegti dirbtinį intelektą įmonėms suteikiant dirbtinio intelekto ženklelį, kuris visiems parodytų jų, kaip savo srities lyderių, padėti; sukurti platformą, per kurią pramonės šakos lyderiai galėtų pristatyti naujoviškus dirbtinio intelekto sistemų panaudojimo savo veikloje būdus; sukurti centrą dirbtinio intelekto startuoliams skatinti ir kt.; viešajame sektoriuje sukurti reguliacinę „smėlio dėžės“ technologija pagrįstą taikomąją programą, leisiančią naudoti ir išbandyti dirbtinio intelekto sistemas viešajame sektoriuje ribotą laiką – taip kūrėjai galėtų išmieginti savo produktą gyvoje aplinkoje, o viešasis sektorius galėtų nuspresti, kokie sprendiniai turėtų būti įdiegti; padėti viešosioms įstaigoms diegti klientams skirtas dirbtinio intelekto sistemas, galinčias sumažinti darbų apimtį; įsteigti Lietuvos dirbtinio intelekto patariamąją valdybą, padėsiančią Vyriausybei priimti sprendimus dėl būsimos dirbtinio intelekto politikos; sukurti viešosios partnerystės pagrindu veikiančias organizacijas, sudarančias geresnes sąlygas dirbtinio intelekto sistemoms vystyti, ir kt.), susitelkti į pagrindinius ekonomikos sektorius, gausiančius daugiausia naudos iš dirbtinio intelekto sistemų pritaikymo; suteikti ateicių su dirbtiniu intelektu reikalingų įgūdžių nuo pat mokinių lavinimo pradžios; suteikti aukštojo mokslo siekiantiems studentams galimybes gilinti žinias dirbtinio intelekto srityje; užtikrinti, kad dabartiniai darbuotojai turėtų besikeičiančiai darbo rinkai reikiamu kompetencijų; pasiekti dirbtinio intelekto sistemų mokslinių tyrimų ir plėtros meistriškumo lygį; sukurti aplinką, skatinančią nuolatinius dirbtinio intelekto tyrimus; sukurti stabilią ir dirbtiniam intelektui palankią duomenų aplinką, pagrindinį dėmesį sutelkiant į viešąjį sektorių; užtikrinti, kad Lietuvos duomenys atitiktų tarpautinių standartų reikalavimus; konsultuoti viešąjį sektorių dėl etiško dirbtinio intelekto reglamentavimo ir įgyvendinimo ir kt.

Didžiosios pasaulio bendrovės, tarp jų ir globaliai veikiančios technologijų milžinės, taip pat pripažįsta strateginę dirbtinio intelekto svarbą, kadangi jo naudojimas padeda mažinti išlaidas, didinti produktyvumą ir išleisti į rinką naujus produktus ir paslaugas. Tuo pat metu sparčiai besikuriančios ir greitai besivystančios naujos technologijų naudojimu grįstos įmonės kelia rimtą konkurenciją tradiciniams verslams, tuo skatindamos šias taip pat neatsilikti nuo technologinių naujovių³⁰.

Plėtoti dirbtinį intelektą ir jo naudojimą siekiant užsistikrinti konkurencingumą pasaulio lygiu yra ir vienas iš Europos Komisijos tikslų. Kaip nurodyta Europos Komisijos baltojoje knygoje „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pa-

³⁰ European Commission/Deloitte, p. 9.

sitikėjimą“, dirbtinis intelektas yra technologijos, kurias taikant derinami duomenys, algoritmai ir kompiuterijos pajėgumai. Todėl kompiuterijos pažanga ir didėjantis duomenų prieinamumas yra pagrindiniai veiksniai, lemiantys dabartinį dirbtinio intelekto pakilimą. Europa gali pasinaudoti savo technologijų ir pramonės pranašumais kartu su kokybiška skaitmenine infrastruktūra ir pagrindinėmis vertybėmis grindžiamą reguliavimo sistema, kad taptų pasauline duomenų ekonomikos ir jos pritaikymo inovacijų lydere. Tuo remdamasi ji gali sukurti dirbtinio intelekto ekosistemą, kurios technologijos būtų naudingos visai Europos visuomenei ir ekonomikai:

- papildoma nauda piliečiams, pavyzdžiui, geresnė sveikatos priežiūra, rečiau gendantį buitinę įranga, saugesnio ir švaresnio transporto sistemos, geresnės viešosios paslaugos;
- plėtros galimybės verslui, pavyzdžiui, naujos kartos produktai ir paslaugos tose srityse, kur Europa yra ypač stipri (mašinos, transportas, kibernetinis saugumas, ūkininkavimas, žalioji ir žiedinė ekonomika, sveikatos priežiūra ir didelės pridėtinės vertės sektorai, pvz., mada ir turizmas), ir
- viešojo intereso paslaugas teikiantiems subjektams, pavyzdžiui, mažesnė (transporto, švietimo, energetikos ir atliekų tvarkymo) paslaugų teikimo kaina, tvaresni produktai ir tinkamos priemonės teisėsaugos institucijoms, piliečių saugumui užtikrinti, kartu taikant tinkamas priemones jų teisėms ir laisvėms apsaugoti³¹.

Kaip minėta, pastaraisiais metais dirbtinio intelekto plėtojimas ir taikymas išaugo labai stipriai. Tai yra vienas didžiausių žmonijos raidos lūžio taškų, pagal savo poveikį neretai gretinamų su pramonės revoliucija, kai rankų darbą pakeitė mašinos. Neabejojama, kad dirbtinio intelekto naudojimas dar labiau plėsis. Tai lemia kelios priežastys. Pirma, tai yra saugojimo ir apdorojimo galios kaina. Fizinių komponentų kainos sumažėjo, o debesų paslaugų teikėjai padarė duomenų debesis prieinamus plačiajai visuomenei. Antra, labai padaugėjo surinktų duomenų. Duomenys iš esmės yra dirbtinio intelekto naudojamų algoritmų statybinė medžiaga. Didėjantis skaitmeninių technologijų (pvz., daugiau išmanijų telefonų) ir nebrangių integruotų įrenginių (pvz., fotoaparatus) paplitimas skatina šį augimą. Be to, nauji metodai leidžia analizuoti nestruktūruotus duomenis, tokius kaip vaizdo įrašas, tekstas ir balsas. Galiausiai, atviri duomenys ne tik didina skaidrumą, bet ir kartu mažina barjerus plėtoti dirbtinį intelektą. Egzistuoja daug žemo kodo sistemų, kuriose galima taikyti ir plėtoti dirbtinio intelekto funkcionalumus³².

Be to, šiuo metu neatrodo, kad sparti dirbtinio intelekto kūrimo ir naudojimo plėtra galėtų sulėtėti. Kaip nurodo Europos Komisija, pagrindinės to priežastys yra:

³¹ Europos Komisija, 2020, p. 2.

³² European Commission/Deloitte, p. 12–13.

1. Techninė pažanga – saugojimo ir apdorojimo galia dvigubėja kas dvejus metus. Be to, sudėtingų algoritmų pažanga vyksta dar greičiau.
2. Ekonominis spaudimas – globalizacija ir kiti veiksniai verčia įmones nuolatos optimizuoti ir siekti naujų išradimų. Įmonės turi panaudoti dirbtinį intelektą, kad išsiltų konkurencingos, teikdamos geresnes paslaugas ir produktus.
3. Politiniai tikslai – daugelis šalių pripažino dirbtinio intelekto potencialą. Daug valstybių skubaapti autoritetu dirbtinio intelekto srityje. Tai matyt ir iš daugybės šalių investicijų bei teisinio reguliacijos, skirto dirbtiniams intelektui³³.

1.4. Dirbtinio intelekto technologiniai sprendimai

Dirbtiniu intelektu gali būti laikomos kompiuterinės sistemos, kurios daro tai, ką „įprastai darytų protinė žmonė“. Tačiau dirbtinis intelektas gali būti pasitelktas ten, kur žmogaus proto nebepakanka. Pavyzdžiu, kai kurių dalykų žmonės negali padaryti patys dėl užduočių ar duomenų sudėtingumo, poreikio greitai suprasti esmę arba dėl to, kad tradiciniai metodai yra neveiksmingi. Pasinaudojant technologijomis ir algoritmais, tokiais, kaip duomenų gavyba, modelių atpažinimas, natūralios kalbos apdorojimas, sukuriamas atsakymas, kokį pateiktų protinges žmogus³⁴.

Dirbtinis intelektas naudojamas kuriant labai įvairias technologijas, kurios taikomos praktikoje. Labiausiai naudojami technologiniai sprendimai yra šie:

Natūralios kalbos apdorojimas. Šis dirbtinio intelekto technologinis sprendimas padeda kompiuteriams suprasti, interpretuoti ir pritaikyti žmogaus kalbą. Kiek anksciau dirbtinis intelektas buvo „išmokytas“ iš esmės tik taisyklių, kaip turi būti atliekamas vertimas, tačiau į natūralios kalbos apdorojimą šiuo metu įtraukiama vis daugiaugiliojo mokymosi elementų, t. y. naudodamos natūralios kalbos apdorojimą mašinos ne tik geba bendrauti su žmonėmis jų gimtaja kalba (t. y. gali skaityti ir girdėti), bet ir gali interpretuoti jų jausmus. Viena pažangiai natūralios kalbos apdorojimo programų yra „Skype Translator“, kuri siūlo tiesioginį vertimą realiuoju laiku į kelias kalbas. Taigi, jei kalba vienas žmogus savo gimtaja kalba, jo tuo pat metu gali klausytis kitis žmonės savo skirtinėmis nacionalinėmis kalbomis.

Vaizdo atpažinimas (paprastai – „Kompiuterinis matymas“ (angl. *Computer Vision*) yra dirbtinio intelekto metodas, padedantis kompiuteriams suprasti vaizdinį pasauly. Ši technologija apdoroja vaizdus ir vaizdo duomenis ir dažniausiai naudoja giliojo mokymosi modelius objektams identifikuoti ir klasifikuoti. Kai sistema perpran-

³³ European Commission/Deloitte, p. 13.

³⁴ European Commission/Deloitte, p. 10.

ta tendencijas, ji gali būti naudojama interpretacijai realiuoju laiku. Pavyzdžiui, kompiuterinis matymas būtinis norint įgalinti savarankiškai važiuojančius automobilius. Įvairūs automobilių gamintojai, pavyzdžiui, „Tesla“, BMW, „Volvo“ ir „Audi“, nauja keliai kameras, radarus ir ultragarsinius jutiklius, siekdami gauti vaizdus iš ap linkos, kad jų savarankiškai važiuojantys automobiliai galėtų aptikti objektus, juostų ženklinimą, ženklus ir eismo signalus tam, kad galėtų saugiai važiuoti³⁵.

Bene plačiausiai naudojamos vaizdo atpažinimo technologijos yra veido atpažinimo technologijos. Veido atpažinimas yra biometrinio tapatybės nustatymo rūšis, kurios metu aptinkamos ir analizuojamos asmens veido ypatybės. Technologija gali būti suskirstyta į keturias kategorijas, priklausomai nuo naudojimo ir tikslų: aptikimas, apibūdinimas, patvirtinimas ir identifikavimas.

- Veido aptikimas. Keliamas klausimas – ar šiame vaizde yra veidų? Šios kategorijos technologijos aptinka veidus nurodytame vaizde. Naudojant šią technologiją nėra individualaus lygmens atitikimo, sistema tiesiog nustato žmogaus veido buvimą pateiktame vaizde ar vaizdo įraše. Šis metodas plačiai naudojamas skaitmeninėse fotokamerose automatiniam aptiktų veidų fokusavimui. Ši technologija nėra tokia sudėtinga, kad būtų galima nustatyti kokias nors būdingas jos aptinkamo veido savybes. Atsižvelgiant į tai, kad jokių lygiu nėra nustatoma tapatybė, vien tik veido aptikimo technologijos naudojimas nekelia jokių su asmens privatumu susijusių problemų.
- Veido apibūdinimas. Keliamas klausimas – ką šie veidai pasako? Ši veido atpažinimo priemonių kategorija analizuojas asmenų fizinę ir emocinę būseną, nei dentifikuojas asmens, bet gali nustatyti tam tikras asmens savybes, pvz., amžių ir lyti. Ši technologija dažniausiai naudojama prekybos centruose, parduotuvėse ir kitose pramogų vietose, kurios nori žinoti tam tikrą demografinę informaciją apie savo klientus.
- Patvirtinimas (1:1). Keliamas klausimas – ar šis asmuo tikrai yra tas, kurio reikia? Patvirtinimas plačiai naudojamas autentifikavimo tikslais. Ši technologija palygina asmens veido duomenis su išanksčiau turimais duomenimis, kad patikrintų, ar dabartinis asmuo yra tokis, koks jis teigia esąs. Ši technologija naujojama atliekant patikrinimus pasienyje, kai dalyvaujančio asmens veidas surerinamas su pateiktais biometriniais duomenimis (pasais ar kitomis biometrinio identifikavimo formomis), ir siekiant saugiai pasiekti įrenginius ar vietas (pvz., mobiliojo telefono atrakinimas).

³⁵ Forbes, 7 Amazing Examples Of Computer And Machine Vision In Practice, 2019. Prieiga per internetą: <https://tinyurl.com/w2mj5vv>.

- Identifikavimas (1:n). Keliamas klausimas – kas yra šis asmuo? Ši technologija naudojama nežinomiems asmenims identifikuoti, lyginant jų veido biometriinius duomenis su esama duomenų baze. Tikrinant 1:1 asmuo identifikuojama save (pvz., pateikia biometrinį pasą pasienio pareigūnui), o sistema patikrina, ar šio konkretaus asmens biometrinis veido kodas yra tokis pat kaip ir jo pateiktame dokumente. Tačiau identifikacijai naudojant 1:n technologijas asmuo nepateikia jokios informacijos ir paprastai net nežino apie technologijos egzistavimą ir naudojimą. Naudojant šią technologiją gautas veido kodas sutikrinamas su duomenų baze, kurioje yra daug (dažniausiai milijonai) veido atvaizdų, siekiant nustatyti asmens tapatybę. Duomenų bazė kuriama naudojant įvairius šaltinius, pvz., įvairius viešuosius registrus (pvz., vairuotojo pažymėjimus ir kitas identifikavimo nuotraukas) ir atviro šaltinio internetinius vaizdus (pvz., socialinės žiniasklaidos ir svetainių vaizdus)³⁶. Ši technologija naudojama tiek socialiniuose tinkluose (pvz., kai gaunami pasiūlymai „pažymeti“ konkretų asmenį ir pasiūlomas jo vardas ir pavardė), tiek ir teisėsaugoje ar migracijos srityje, kai siekiama identifikuoti konkrečius (galimai nusikalstamą veiką padariusius) asmenis³⁷.

Kalbos atpažinimas yra dirbtinio intelekto metodas, kai kompiuteris atpažista ištartus žodžius, t. y. natūralią žodinę kalbą. Jis paverčia akustinį signalą rašytiniais žodžiais. Šis metodas gali būti naudojamas kartu su natūralios kalbos apdorojimu, kaip apibūdinta aukščiau, kai yra apdorojama ištartu žodžiu reikšmė. Kalbos atpažinimas šiuo metu jau naudojamas labai plačiai, pvz., juo grindžiamos tokios programos kaip „Siri“ ir „Amazon Alexa“.

Ekspertinės sistemos (angl. *Expert Systems*) yra viena iš sukurtų taikomujų programų, naudojančių dirbtinį intelektą sudėtingoms konkrečios srities problemoms spėsti, kai yra sukonzentruojamos žinios ir patirtis, o to žmogus nepajėgus atliki savo jégomis. I modelį integruojamos aukštos kokybės žinios iš įvairių tos srities ekspertų. Be to, sistemoje yra vadinančios išvadų variklis (angl. *inference engine*), kuriam padedant išskaičiuojami teisingi arba geriausi sprendimai. Vienas iš šių sistemų trūkumų

³⁶ Pvz., žr. Olivia Solon. Facial Recognition's 'Dirty Little Secret': Millions Of Online Photos Scrapped Without Consent. *NBC News*, 2019, 12 March. Prieiga per internetą: www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921; Olivia Solon & Cyrus Farivar. Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop Facial Recognition Tools. *NBC News*, 2019, 9 May. Prieiga per internetą: www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

³⁷ Pipedas, C. 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation Against Facial Recognition Technology. *Canadian Journal of Law and Technology*, 2020, June, p. 4–5.

yra sunkumai gauti, įvesti ir atnaujinti žinias šiame modelyje. Tokios sistemos pavyzdys yra PXDES, naudojamas plaučių vėžio laipsniui ir tipui numatyti^{38,39}.

1.5. Dirbtinio intelekto naudojimas privačiame ir viešajame sektoriuose

Šiuo metu dirbtinis intelektas naudojamas labai įvairiose srityse, tačiau tik pastaraisiais metais galima ižvelgti nuoseklų dirbtinio intelekto sistemų diegimą į tam tikras privataus ir viešojo sektoriaus veiklos sritis. Remiantis „Deloitte“, galima išskirti pagrindines šešias tendencijas:

- Dirbtinio intelekto naudojimas kuriant strategijas – dirbtinio intelekto padedamos organizacijos kuria naujas koncepcijas, paslaugų variantus, atveria naujus produktus ir rinkas.
- Dirbtinio intelekto diegimas į organizacijų procesus. Kadangi dirbtinio intelekto galimybės plečiasi atliekant įvairias užduotis, organizacijos nustato, kaip sprendimus priimantys žmonės sąveikauja su algoritmais ir juos valdo.
- Darbuotojų įtraukimas į dirbtinio intelekto „mokymą“ – žmonės, kurių darbe yra mažiau techninių užduočių, pvz., vadovai ir procesų savininkai, gali dalyvauti kuriant dirbtinį intelektą.
- Duomenų rinkimo ir naudojimo tobulinimas. Dirbtinis intelektas sudaro geresnes galimybes tiek rinkti, tiek analizuoti vaizdinius, garsinius ir nestruktūruotus duomenis, ir tai leidžia organizacijoms rasti naujų įžvalgų.
- Vis augantis technologijų naudojimas – atvirojo kodo algoritmai, nebrangios platformos ir perėjimas prie debesies reiškia, kad dirbtinio intelekto pritaikymas yra greitesnis ir lengvesnis, ypač mažesniems rinkos dalyviams.
- Etikos standartų naudojant dirbtinį intelektą diegimas – organizacijos skiria dėmesį etikos problemoms ir užtikrina aukštésnius dirbtinio intelekto naudojimo standartus⁴⁰.

Kalbant apie privatų sektorių, vis daugiau privačių įmonių diegia dirbtinio intelekto elementus į kasdienių funkcijų vykdymą, prekių gamybą bei paslaugų teikimą. Dirbtinis intelektas privačiame sektoriuje patrauklus dėl gebėjimo santiokinai mažais kaštais gerinti klientų patirtį, skatinti pardavimus remiantis duomenimis grįstais

³⁸ Medium, Expert Systems and Applied Artificial Intelligence, 2018. Prieiga per internetą: <https://tinyurl.com/y6demvgt>.

³⁹ European Commission/Deloitte, p. 189, OECD, 2019.

⁴⁰ European Commission/Deloitte, p. 192.

skaičiavimais ir t. t. Didėjantį poreikį gerinti klientų patirtį lemia intensyvi konkurenčija rinkoje, o tai atlikti padeda personalizavimo galimybės. Dirbtinis intelektas jau daugelyje įmonių naudojamas siekiant personalizuoti pardavimus bei teikti klientų aptarnavimo paslaugas, ir prognozuojamas dirbtinio intelekto naudojimo šiose srityse didėjimas. Šiuo metu dar skirtingai nuo to, kas vaizduojama mokslinės fantastikos filmuose, dirbtinis intelektas daugiau naudojamas vidiniuose įmonių procesuose siekiant didinti efektyvumą, organizuoti darbus ir didinti produktyvumą. Pagrindiniai dirbtinio intelekto naudojimo privačiose įmonėse būdai yra šie:

- *Personalizavimas.* Pasitelkiant dirbtinį intelektą gerinama klientų patirtis teikiant suasmenintus pasiūlymus. Pavyzdžiu, pardavėjai gali teikti rekomendacijas dėl prekių ir paslaugų remdamies ankstesne klientų patirtimi ir jų interesais; socialinės medijos platformos gali naudoti personalizavimą siekdamos nustatyti, kokį turinį reikėtų rodyti naudotojams⁴¹; klientų aptarnavimo srityje kompiuteriniai robotai raštu ir žodžiu bendrauja su klientais ir t. t.
- *Procesų automatizavimas.* Dirbtinis intelektas ypač naudingas automatizuojant tam tikrus verslo procesus, naudojant vadinančią robotinį procesų automatizavimą (angl. *robotic process automation* (RPA)). Nemažai didžiujų pasaulinių lygiu veikiančių įmonių naudoja robotinį procesų automatizavimą organizuodamos savo funkcijų vykdymą⁴².
- *Klientų aptarnavimas.* Šiuo metu daug prekybos įmonių pardavinėja prekes netik fizinėse parduotuvėse, bet ir intername. Kuriasi nemažai parduotuvių, veikiančių tik intername. Kadangi internetu perkantys klientai susiduria su įvairiais klausimais ir sunkumais įsigyjant prekes ar paslaugas, pardavėjai, siekdami kuo sklandžiau atliepti klientų poreikius ir gerinti jų pirkimo patirtį, įdarbina dirbtinį intelektą. Tam naudojamos tokios priemonės, kaip pokalbių robotai arba įvairūs klientų poreikius tenkinantys klientų aptarnavimo kanalai⁴³.
- *Didinamas produktyvumas.* Nemažai pasaulyje lyderiaujančių bendrovių naudoja dirbtinį intelektą siekdamos didinti gamybos apimtis per trumpesnį laiką. Pavyzdžiu, „Nissan“ bando naudoti dirbtinį intelektą kurdama naujus mode-

⁴¹ Pvz., žr. Smart Data Collective. How Netflix Is Using Artificial Intelligence And Big Data To Drive Business Performance. Prieiga per internetą: <https://www.smartdatacollective.com/how-netflix-is-using-artificial-intelligence-and-big-data-to-drive-business-performance/>.

⁴² AskeyGeek. Companies using Robotic Process Automation. Prieiga per internetą: <https://www.askeygeek.com/companies-using-robotic-process-automation/>.

⁴³ Pvz., žr. TechGig. Here's how Amazon is using AI to improve customer support. Prieiga per internetą: <https://content.techgig.com/heres-how-amazon-is-using-ai-to-improve-customer-support/articleshow/-74381649.cms>.

lius realiu laiku, siekdama sutrumpinti laiko tarpą nuo modelio sukūrimo iki pardavimo⁴⁴.

- *Duomenų analizė.* Viena iš sričių, kur šiuo metu dirbtinis intelektas pasitelkiamas plačiausiai, yra duomenų analizė. Pavyzdžiui, „Google“ naudoja labai įvairius duomenų šaltinius ir atlieka turimų duomenų nuspėjamąjį analizę⁴⁵. Tarkime, „Google“ bendrovės, remdamosis asmens namų adresu, kalendoriaus įrašais ir žemėlapio informacija, gali pasakyti, kad laikas išvykti į oro uostą, jei norima suspėti į skrydį, įmonės vis dažniau gali pasinaudoti kontekstine informacija savo įmonėje. Analitikos automatizavimas – dažnai vadinamas išmaniuoju duomenų aptikimu (angl. *smart data discovery*) arba išplėstine analize (angl. *augmented analytics*) – sumažina žmogaus patirties ir sprendimų poreikių, nes automatiškai nurodo duomenų ryšius ir modelius. Kai kuriais atvejais sistemos netgi rekomenduoja, ką vartotojas turėtų daryti, kad išspręstų tam tikrą situaciją, kurią nustato automatizuota analitika⁴⁶.

Viešajame sektoriuje poreikis plėtoti dirbtinį intelektą ir naudotis jo teikiamomis galimybėmis panašus į privataus sektorius. Valstybės institucijos naudoja ar ketina naudoti dirbtinį intelektą tiek savo vidaus procesų optimizavimui, tiek interesantų aptarnavimo srityje. Nors viešosios valdžios institucijos yra labiau suinteresuotos užtikrinti procesų stabilumą ir atliepti piliečių ir gyventojų poreikius, o ne orientuojasi į pardavimų apimčių didinimą, piliečiai ir kiti interesantai vis dėlto tikisi pažangiu inovacijų ir viešajame sektoriuje, panašių į tas, kurių galėtų tikėtis iš privataus sektoriaus įmonių. Taikydamos naujas technologijas, vyriausybės gali integruoti įvairių viešųjų paslaugų teikimą, taip gerindamos gyventojų patirtis. Vienas tokų integracijos pavyzdžių galėtų būti skaitmeninė tapatybė – Estijos skaitmeninė infrastruktūra viešojo sektorius subjektams lengvai identifikuoti piliečius ir efektyviai siūlyti paslaugas. Pagrindinė piliečių informacija įvedama tik vieną kartą ir šie duomenys naudojami teikiant įvairias viešasias paslaugas, tokias, kaip mokesčių surinkimas, sveikatos apsauga, balsavimas ir t. t.⁴⁷

Šiuo metu viešajame sektoriuje dirbtinis intelektas daugiausia taikomas siekiant efektyvinti valstybės tarnautojų kasdienį darbą, mažinti ar iš viso panaikinti besikar-

⁴⁴ Forbes. 10 Ways AI Is Improving Manufacturing in 2020. Prieiga per internetą: <https://www.forbes.com/sites/louiscolumbus/2020/05/18/10-ways-ai-is-improving-manufacturing-in-2020/?sh=3bebcd5f1e85>.

⁴⁵ CompTIA. Using AI in Business: Examples of Artificial Intelligence Application in Business. Prieiga per internetą: <https://connect.comptia.org/blog/using-ai-in-business>.

⁴⁶ Davenport, T., Fitts, J. AI Can Help Companies Tap New Sources of Data for Analytics. *Harvard Business Review*, 2021, March 19. Prieiga per internetą: <https://hbr.org/2021/03/ai-can-help-companies-tap-new-sources-of-data-for-analytics>.

⁴⁷ Deloitte US. The digital citizen, 2019. Prieiga per internetą: <https://tinyurl.com/vykd76qc>.

tojančius darbus, kuriuos atlieka valstybės tarnautojai, kad šie galėtų imtis kūrybiškesnių ar strateginių užduočių⁴⁸. Remiantis mokslininkų Viechnicki ir Eggers'o atliktu tyrimu, valstybės tarnautojas vidutiniškai 30 proc. savo darbo laiko praleidžia dokumentuodamas informaciją ir atlikdamas kitus įprastus administracinius darbus⁴⁹. Jei tokios užduotys būtų bent iš dalies automatizuotos, viešosios valdžios institucijos galėtų surūpinti nemažai pinigų, perkvalifikuoti valstybės tarnautojus atlikti svarbesnes užduotis, o tai kartu didintų galimybes iš viešajų sektorų pritraukti daugiau kvalifikuotų darbuotojų⁵⁰. Nacionalinės ir vietos valdžios institucijos glaudžiai bendradarbiauja su mokslininkais ir pramonės lyderiais siekdamos įdiegti pažangias dirbtinio intelekto technologijas į įvairias viešosios politikos sritis – koordinuojant transporto eismą, skaitmeninant institucijų ir įstaigų dokumentų tvarkymą, taip pat specifinėse švietimo, sveikatos apsaugos, socialinės apsaugos srityse. Kai kurios valstybės (pvz., Danija) naudoja dirbtiniu intelektu pagrįstas nuspėjamąsias programas siekdamos įvertinti kandidatus, pretenduojančius į valstybės teikiamas dotacijas ir socialines išmokas⁵¹.

Sienų apsauga. Viena iš viešojo sektoriaus sričių, kur dirbtinis intelektas naudojamas itin didele apimtimi, yra valstybių sienų apsauga. Sienų apsaugos valdymas yra susijęs su įvairiu viešojo sektoriaus institucijų ir įstaigų, veikiančių muitinės, sienų kontrolės, aviacijos saugumo, teisėsaugos, imigracijos, vizų išdavimo ir tvarkymo ir kt. srityse, veikla. Vykstant globalizacijai, prekių ir gyventojų judėjimas per sienas įgauna precedento neturintį mastą. Todėl vyriausybės ieško skaitmeninių sprendimų ir plėtoja pažangiausias technologijas, kad greičiau ir kokybiškiau prisitaikytų prie migracijos tendencijų⁵².

Apsauga nuo terorizmo. Dirbtinio intelekto priemonės gali padėti geriau apsaugoti ES piliečius nuo nusikaltimų ir teroro aktų. Pavyzdžiu, jos gali padėti atpažinti terorizmo propagandą internete, nustatyti įtartinus pavojingų produktų pardavimo sandorius, aptikti pavojingus slepiamus daiktus, neteisėtas medžiagas ar produktus, teik-

⁴⁸ OECD, p. 77.

⁴⁹ Viechnicki, P., Eggers, W. D. *How much time and money can AI save government? Cognitive technologies could free up hundreds of millions of public sector worker hours.* Deloitte University Press, 2018. Prieiga per internetą: https://www2.deloitte.com/content/dam/insights/us/articles/3834_How-much-time-and-money-can-AI-save-government/DUP_How-much-time-and-money-can-AI-save-government.pdf.

⁵⁰ Partnership for Public Service/IBM Center for the Business of Government. *The Future Has Begun.* Washington, DC, 2018. Prieiga per internetą: <https://ourpublicservice.org/publications/the-future-has-begun-using-artificial-intelligence-to-transform-government/>.

⁵¹ European Commission/Deloitte, p. 19.

⁵² European Commission/Deloitte, p. 18.

ti pagalbą piliečiams ekstremaliosiose situacijose ir susiorientuoti pirmojo reagavimo pajėgomis⁵³.

Sveikatos apsauga. Dirbtinis intelektas jau yra naudojamas sveikatos priežiūros srityje, bet netolimoje ateityje jo panaudojimą ketinama dar daugiau išplėsti. Dirbtinio intelekto programos, grindžiamos mašininiu mokymusi, gali padėti interpretuoti rezultatus, nustatyti preliminarias diagnozes, rizikos veiksnius ir galimas preventines priemones. Atsižvelgiant į tai, kad dirbtinis intelektas gali apdoroti labai daug individualių duomenų, mašininio mokymosi būdu dirbtinis intelektas gali padėti gydytojams individualizuoti gydymą pagal labai įvairius pacientų duomenis. Taigi, kartu su ekspertinėmis gydytojų žiniomis, dirbtinis intelektas gali padėti siekti didesnio tikslumo, efektyvumo bei sudaryti salygas gauti daugiau pageidaujamų rezultatų sveikatos apsaugos srityje⁵⁴. Pavyzdžiui, dirbtinis intelektas naudojamas gydant vėžį. Plaučių vėžys yra viena iš pagrindinių su vėžiu susijusių mirčių priežasčių ir šią vėžio formą labai svarbu diagnozuoti kuo anksčiau. „Google“ ir „Northwestern Medicine“, mokslinis medicinos centras Čikagoje, bendradarbiavo kurdami giliojo mokymosi dirbtinio intelekto algoritmą, skirtą peržiūrėti anksčiau skenuotus vaizdus, kuriais buvo diagnozotas plaučių vėžys. Vėliau algoritmas pats vertino skenuotas nuotraukas siekdamas nustatyti, ar jose matyti vėžio požymį. Tyrėjai palygino dirbtinio intelekto prognozes su radiologų, turinčių didelę patirtį šioje srityje, nuomone ir paaškėjo, kad dirbtinio intelekto sistemos buvo arba tiek pat tikslios, arba tikslesnės nei gydytojų prognozės⁵⁵.

Transportas. Dirbtinis intelektas plačiai naudojamas kuriant autonomines transporto priemones, tačiau tai daugiau privataus sektorius iniciatyvos, siekiant suteikti vartotojams daugiau patogumo. Viešajame sektoriuje dirbtinis intelektas daugiau naudojamas valdant transporto srautus ir užtikrinant saugumą keliuose. Pavyzdžiui, Portugalijoje Lisabonos miesto taryba, bendradarbiaudama su Nacionaline civilinės inžinerijos laboratorija ir Aukštuoju technikos institutu, įdiegė dirbtinio intelekto sistemas, padedančias rinkti, apdoroti, sugrupuoti ir naudoti miesto judėjimo ir susijusių aplinkybių duomenis, siekiant struktūruoti ir integruotai valdyti eismo srautus. Taip pat Portugalijoje dirbtinis intelektas naudojamas siekiant sumažinti greitosios medicinos pagalbos automobilių judėjimo laiką. Tam buvo kuriami nuspėjamieji modeliai,

⁵³ Europos Komisijos komunikatas „Europos žaliasis kursas“. COM(2019) 640 final.

⁵⁴ Ubaldi, B., Le Fevre, E. M., Petrucci, E., Marchionni, P., Biancalana, C., Hiltunen, N., Intravaia, D. M., Yang, C. State of the art in the use of emerging technologies in the public sector. *OECD Working Papers on Public Governance*, 2019, No. 31. OECD Publishing, Paris.

⁵⁵ Sandoiu, A. Artificial intelligence better than humans at spotting lung cancer. *Medical News Today*, 2019, May 20. Prieiga per internetą: www.medicalnewstoday.com/articles/325223.php.

naudojant istorinius duomenis apie judėjimo greitį bei įvairius kontekstinius duomenis iš kelių šaltinių (pvz., oro sąlygos)⁵⁶.

Saugumo ir teisingumo užtikrinimas. Saugumo srityje dirbtinis intelektas naudojamas užtikrinant tiek fizinį, tiek kibernetinį saugumą ir apima daug įvairių sričių, tokį kaip teisėsaugos institucijų veikla, nelaimingų atsitikimų prevencija ir padarinių likvidavimas, karinis ir nacionalinis saugumas. Saugumo užtikrinimo tikslu naudojamos viešų erdvų ir objektų vaizdo stebėjimo programos, tačiau taip pat pradedamos naudoti kompiuterinio matymo ir natūralios kalbos apdorojimo sistemos, kurios leidžia apdoroti didelius vaizdo, teksto ir kalbos duomenis, nustatyti grėsmes visuomenės saugumui realiuoju laiku. Veido atpažinimo technologijos taip pat naudojamos daugelyje didžiųjų pasaulio miestų siekiant nustatyti įtariamus nusikalstelius ir kovojant su terorizmu. Kaip bus aptarta vėliau, šis dirbtinio intelekto naudojimas yra vienės prieštaragingiausių ir glaudžiai susijęs su galimu žmogaus teisių, ypač teisés į privatumą, pažeidimu⁵⁷. Policijos srityje didelio duomenų kiekiečių analizė padeda atlkti nusikalstamų veikų tyrimus, taip pat iš anksto prognozuoti galimas nusikalstamas veikas bei palengvina vietovių ir objektų stebėjimą realiuoju laiku⁵⁸.

Santykiai su gyventojais ir verslo subjektais. Viešosios valdžios institucijos pasitelkia intelektą siekdamos užtikrinti kokybišką ir efektyvų bendravimą su gyventojais ir verslo subjektais. Vienas populiariausiai dirbtinio intelekto naudojimo viešajame sektoriuje būdų yra pokalbių robotai. Panašiai kaip ir privačių organizacijų naudojami pokalbių robotai, jie gali būti paprastesni, t. y. užprogramuojami atsakyti į dažniausiai keliamus klausimus, arba sudėtingesni, grindžiami mašininiu mokymusi, kai sudaromos galimybės atsakyti į sudėtingesnius klausimus bei valdyti platesnio pobūdžio pokalbius⁵⁹. Vienas iš dirbtinio intelekto naudojimo viešajame sektoriuje siekiant pagerinti viešąsias paslaugas verslui pavyzdžiu galėtų būti Latvijos įmonių registro sistema UNA, t. y. 24/7 veikiantis virtualus pagalbinis pokalbių robotas, kuris teikia rašytinius atsakymus į dažniausiai užduodamus klausimus suinteresuoju siems asmenims, išskaitant pateiktų dokumentų statuso atnaujinimą. UNA gali būti pasiekama per Latvijos įmonių registrą bei „Facebook Messenger“ programėlę. Ši sistema sumažina poreikį „gyvai“ atsakinėti į didelį srautą panašių užklausų telefonu ar atvykus tiesiogiai. Įmonių registro darbuotojai nuolat „moko“ UNA papildomų klausimų ir atsakymų, kad ji galėtų pateikti dar išsamesnius atsakymus. Per pirmuosius veikimo metus UNA atsakė į daugiau nei 22 000 klausimų iš beveik 4000 naudotojų. Latvijos įmonių regist-

⁵⁶ OECD, p. 79–80.

⁵⁷ Ubaldi et al.

⁵⁸ European Commission/Deloitte, p. 19.

⁵⁹ OECD, p. 81–82

1. DIRBTINIO INTELEKTO ŠAMPRATA IR NAUDΟJIMAS VISUOMENĖS GYVENIME

ras taip pat svarsto galimybę naudoti UNA kaip mokymų programą naujiems darbuotojams⁶⁰.

Dirbtinis intelektas viešajame sektoriuje taip pat naudojamas teisėkūroje, teismų darbe, aplinkosaugos, energetikos srityse⁶¹.

Apibendrinant galima teigti, akivaizdu, kad dirbtinis intelektas yra vienas svarbiausių pastarųjų metų technologinių sprendimų, leidžiančių žmonijai iš esmės keisti įprastas darbo rutinas, spartinti gamybą, gyventojų aptarnavimą, viešujų paslaugų teikimą, optimizuoti viešajį ir privatų gyvenimą. Galima ižvelgti labai daug dirbtinio intelekto sistemų teikiamų privalumų įvairiausiose privataus ir viešojo gyvenimo srityse. Sparti dirbtinio intelekto technologijų plėtra rodo, kad tai, kiek dirbtinio intelekto kūrimas ir naudojimas yra aktualus dabar, po kelerių metų gali būti nebeaktualu, kadangi bus kuriami ir praktikoje naudojami nauji modeliai, dirbtinis intelektas bus pritaikomas vis įvairesnėse srityse. Atsižvelgiant į tokį dirbtinio intelekto progresą ir jo naudą valstybėms, visuomenei ir atskiriems asmenims yra akivaizdu, kad šiuo atveju riboti interneto plėtrą teisiniais ribojimais būtų ne tik netikslinga, bet ir nuostolina, ypač atsižvelgiant į pasaulinę dirbtinio intelekto plėtrą. Vietoje to, teisė turi prisitaikyti prie technologinių naujovių ir nustatyti saugiklius, kad žmogaus teisės jas naujodant nebūtų pažeidžiamos. Atsižvelgiant į tai, kituose šios studijos skyriuose bus analizuojama, kokias grėsmes dirbtinis intelektas kelia žmogaus teisėms, ypač teisei į privatumą ir duomenų apsaugą, bei vertinama, kokiais teisiniais instrumentais šios grėsmės galėtų būti suvaldomos.

⁶⁰ OECD, p. 82.

⁶¹ OECD, p. 82–87.

2. DIRBTINIO INTELEKTO NAUDOJIMO KELIAMOS GRĖSMĖS VISUOMENEI IR INDIVIDAMS

Kaip apibūdinta ankstesniame skyriuje, dirbtinis intelektas plačiai naudojamas labai įvairiose visuomenės gyvenimo srityse, ir neabejotina, kad dirbtinio intelekto nauojimas tik didės ir sudėtingės. Tačiau tiek privačios bendrovės, tiek ir įvairių valstybių vyriausybės pripažista kartu su dirbtinio intelekto naudojimu ir plėtra neišvengiamai kylančias rizikas. Kaip bus apibūdinta toliau, šiuo metu aktualiausios problemas, atsirandančios su dirbtinio intelekto diegimu įvairiuose procesuose, yra susijusių su galimais saugumo, skaidrumo, privatumo, atskaitingumo ir kontrolės pažeidimais ar trūkumu. Tačiau atsižvelgiant į tai, kad dirbtinis intelektas yra nuolat tobulinamas ir jo veikimo principai sudėtingėja, labai tikėtina, kad iškils ir naujų rizikų pavyzdžiui, susijusių su autonominiu dirbtinio intelekto veikimu (pavyzdžiui, jau buvo pastebėta, kad savaeigės mašinos kelia grėsmę tiek jų naudotojams, tiek ir aplinkiniams asmenims)⁶².

Susirūpinimą dėl dirbtinio intelekto keliamų grėsmių išreiškė ir Europos Parlamento nariai, nurodydami, jog dirbtinio intelekto naudojimas viešojoje politikoje gali vesti prie masinio sekimo pažeidžiant pagrindinius ES proporcingumo ir būtinumo principus. Jie teigia, jog būtina užtikrinti, kad dirbtinio intelekto sistemos būtų prižiūrimos atsakingų asmenų, naudojami algoritmai būtų vieši ir atliekami juos naudojančių dirbtinio intelekto sistemų auditai; kad privačios veido atpažinimo duomenų bazės, elgesio standartais grindžiamos teisėsaugos taisyklės bei asmenų reitingavimas būtų uždrausti ir kad sienų apsaugos kontrolės metu nebūtų naudojamos automatiizuotos atpažinimu grindžiamos sistemos⁶³. Ši Europos Parlamento narių iniciatyva atrodo išties neįprastai viso dirbtinio intelekto Europoje politinio vertinimo kontekste – atvirkščiai, tiek Europos Komisija, tiek atskiro valstybės yra linkusios kuo labiau skatinti ir remti dirbtinio intelekto technologinę plėtrą ir pritaikomumą visuomenės gyvenime.

⁶² European Commission/Deloitte, p. 9.

⁶³ European Parliament. Artificial Intelligence in policing: safeguards needed against mass surveillance. Prieiga per internetą: <https://www.europarl.europa.eu/news/en/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance>.

Tačiau nors dirbtinio intelekto plėtra yra skatinama valstybiniu, regioniniu ir pa-saulio lygiu, ir politikai, ir mokslininkai pabrēžia būtinumą atsižvelgti ir į dirbtinio intelekto keliamas rizikas ir grēsmes žmogaus teisēms. Pavyzdžiui, 2019 metais Euro-pos Tarybos Automatizuoto duomenų tvarkymo ir įvairių dirbtinio intelekto formų žmogaus teisių ekspertų komitetas (angl. *Expert Committee on Human Rights Dimensions of Automated Data Processing and Different forms of AI* (MSI-AUT)) nurodė, kad algoritmais grindžiamos sprendimų priėmimo sistemos, kurios remiasi duome-nimis grįstomis profiliavimo technikomis, gali kelti grēsmę keletui žmogaus teisių, išskaitant teisę į teisingą teismą ir tinkamą procesą, teisę į saviraiškos ir informacijos laisvę bei teisę į privatumą ir asmens duomenų apsaugą⁶⁴. 2020 m. balandžio mėnesį priimtos Europos Tarybos rekomendacijos dėl algoritminių sistemų poveikio žmo-gaus teisēms nurodo, kad algoritminių sistemų naudojimas kasdieniame gyvenime kelia didelę grēsmę žmogaus teisēms, išskaitant teisę į teisingą teismą, teisę į privatumą ir asmens duomenų apsaugą, teisę į minties, sąžinės ir religijos laisvę, teisę į saviraiš-kos laisvę, teisę į susirinkimų laisvę, teisę į vienodų sąlygų užtikrinimą ir socialines bei ekonomines teises. Bendrai sutariama, kad dirbtinio intelekto sistemos, naudoja-mos teisėsaugos ir baudžiamosios justicijos srityse, gali kelti dar didesnę grēsmę žmo-gaus teisių užtikrinimui.

Kaip nurodoma Europos Komisijos baltojoje knygoje „Dirbtinis intelektas. Euro-pos požiūris į kompetenciją ir pasitikėjimą“, dirbtinio intelekto naudojimas gali daryti poveikį pamatinėms ES vertybėms ir pažeisti pagrindines teises, išskaitant teisę į sa-viraiškos laisvę, susirinkimų laisvę, žmogaus orumą, nediskriminavimą dėl lyties, ra-sinės arba etninės kilmės, religijos ar tikėjimo, negalios, amžiaus arba seksualinės orientacijos, kai tai aktualu tam tikrose srityse, teisę į asmens duomenų ir privatumo apsaugą arba teisę į veiksmingą teisminę gynybą ir teisingą bylos nagrinėjimą, taip pat neatitikti vartotojų apsaugos taisyklių. Ši rizika gali kilti dėl to, kad yra bendrujų dirbtinio intelekto sistemų projektavimo trūkumų (be kita ko, susijusių su žmogaus atliekama priežiūra), arba dėl to, kad naudojami neobjektyvūs duomenys (pvz., siste-mai mokyti naudojami tik arba daugiausia vyrų duomenys, todėl moterų atžvilgiu gau-nami neoptimalūs rezultatai). Šioje baltojoje knygoje nurodoma, kad dirbtinis intelektas gali atliliki daug funkcijų, kurias anksčiau galėjo atliliki tik žmogus. Todėl tiek gyventojai, tiek privačios įmonės ar valstybės institucijos vis dažniau susidurs su veiks-mais ir sprendimais, kurie bus priimami dirbtinio intelekto sistemų arba jomis nau-

⁶⁴ Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT), Responsibility and AI: A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework (Rapporteur: Karen Yeung), DGI(2019)05, Council of Europe, September 2019.

dojantis ir kuriuos kartais gali būti sunku suprasti bei prireikus veiksmingai užgincyti. Be to, dirbtinis intelektas suteikia daugiau galimybių stebeti ir analizuoti kasdienius žmonių įpročius. Pavyzdžiu, esama rizikos, kad valstybės institucijos ar kiti subjektai, pažeisdami ES duomenų apsaugos ir kitas taisykles, gali naudoti dirbtinį intelektą masinio sekimo tikslais, o darbdaviai gali stebeti, kaip elgiasi jų darbuotojai. Analizuojant didelius duomenų kiekius ir nustatant jų sąsajas, dirbtinis intelektas taip pat gali būti naudojamas asmens duomenims atsekti ir išanonominti, taip išskiltų naujo pobūdžio pavojas asmens duomenų apsaugai net ir tada, kai pačiuose duomenų rinkiniuose asmens duomenų nėra. Interneto tarpininkai taip pat naudoja dirbtinį intelektą siekdami nustatyti naudotojus dominančios informacijos prioritetus ir parinkti jiems turinį. Tai, kaip tvarkomi duomenys, projektuoamos prietaikos ir kokią galimybę įsikišti turi žmogus, gali turėti įtakos teisėms į saviraiškos laisvę, asmens duomenų apsaugą bei privatumą ir politinėms laisvėms⁶⁵.

Kai kuriems dirbtinio intelekto algoritmams, naudojamiems nusikaltimų recidyvui prognozuoti, gali būti būdingas neobjektyvumas lyties ar rasės pagrindu, dėl kurio skirtingai nustatoma moterų ir vyrų arba piliečių ir užsieniečių recidyvo tikimybė⁶⁶.

2.1. Diskriminacija ir šališkumas

Kaip teigia Cassie Kozyrkov, šališkumas atsiranda ne iš dirbtinio intelekto algoritmų, o iš žmonių⁶⁷. Išties, dirbtinio intelekto veiklos modelis, ar tai būtų mašininis mokymasis, ar gilusis mokymasis, yra kildinamas arba iš žmogaus suformuluotų taisyklų, arba iš atlirkų veiksmų ar visuomenės gyvenimo tendencijų.

Anksčiau minėtoje Europos Komisijos baltojoje knygoje „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ nurodoma, kad šališkumas ir diskriminacija yra bet kuriai visuomeninei ar ekonominėi veiklai būdinga rizika. Žmogus, priimdamas sprendimus, nėra apsaugotas nuo klaidų ir neobjektyvumo. Tačiau dirbtinio intelekto neobjektyvumo padariniai galėtų būti kur kas didesni, dėl jo gali nukenčiami ir būti diskriminuojami daug žmonių, nes nėra socialinės kontrolės mechanizmų reguliuojančių žmonių elgesį. Taip gali atsitiktii ir tada, kai dirbtinio intelekto sistema

⁶⁵ Europos Komisija, 2020, p. 11–12.

⁶⁶ Tolan, S., Miron, M., Gomez, E., Castillo, C. *Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia*. Best Paper Award, International Conference on AI and Law, 2019; Buolamwini, J., Gebru, T. Proceedings of the 1st Conference on Fairness, Accountability and Transparency. *PMLR*, 2018, No. 81.

⁶⁷ Kozyrkov, C. *What is Bias?* Prieiga per internetą: <https://towardsdatascience.com/what-is-ai-bias-6606a3bcb814>.

vienu metu ir veikia, ir „mokosi“. Tais atvejais, kai nepageidaujamų rezultatų negaliama išvengti ar numatyti projektavimo etape, rizika kyla ne dėl pirminio sistemos projekto trūkumų, o dėl praktinio koreliacijų ar dėsningumų, kuriuos sistema nustato iš didelio duomenų rinkinio, poveikio. Dėl daugeliui dirbtinio intelekto technologijoms būdingų ypatybių, tokį kaip neskaidrumas, sudėtingumas, nenuuspėjamumas ir (dažnus) autonomišumas, gali būti sunku patikrinti jų atitiktį galiojančių ES teisės aktų, kuriais siekiama apsaugoti pagrindines teises, taisyklėms ir tai gali trukdyti veiksmingai užtikrinti jų vykdymą. Vykdymo užtikrinimo institucijoms ir poveikį patyrusiems asmenims gali trūkti priemonių patikrinti tai, kaip tam tikras sprendimas buvo priimtas naudojant dirbtinį intelektą, taigi ir tai, ar laikytasi atitinkamų taisyklių. Dėl tokų sprendimų nukentėjusiems fiziniams ir juridiniams asmenims gali kilti sunkumų veiksmingai pasinaudoti teise kreiptis į teismą⁶⁸.

Pavyzdžiui, ir su veido atpažinimo technologijų naudojimu susiję algoritmai gali lemti diskriminaciją ir tendencingumą. Yra įsivyravusi pavojinga nuostata, kad dirbtinio intelekto technologijos yra neutralios ir objektyvios, ir dėl to jas reikėtų naudoti daugiau nei žmogiškajį indėlį priimant sprendimus. Algoritmai kuriami remiantis tam tikru metu egzistavusiais visuomenės elgsenos duomenimis, kurie implikavo tam tikrų taisyklių sukūrimą. Tačiau visuomenė nuolat keičiasi, ir tai yra svarbus veiksnys, dėl ko „senieji“ algoritmai nebetenka savo aktualumo. Dėl to teigiamo, kad yra būtinas žmogaus įsikišimas ar priežiūra, kad šie algoritmai būtų naudojami teisingai. To nesant, net ir esant geriem ketinimams, dirbtinio intelekto algoritmais grindžiama sistema gali būti diskriminuojanti, nepagrįstai riboti asmenų privatumą ir daryti neteisingas išvadas. Pavyzdžiui, didelė grėsmė būti diskriminuojamiams atsiranda tam tikroms mažumoms. Pavyzdžiui, jei prieš tam tikrą laikotarpį vyrai ir juodaodžiai statistiškai daugiau buvo linkę nusikalsti, tai nereiškia, kad, praėjus keliems dešimtmeciams, visuomenės situacija bus išlikusi tokia pati. Taigi, atsižvelgiant į dirbtinio intelekto algoritmų nelankstumą, yra didelė tikimybė, kad pasikeitus visuomenės situacijai tam tikros grupės žmonių patirs dirbtiniu intelektu pagrįstą diskriminaciją.

2.2. Susirinkimų laisvės galimi suvaržymai ir masinio sekimo grėsmės

Dirbtinis intelektas, išskaitant veido atpažinimo technologijas, plačiai naudojami užtikrinant saugumą tiek privačiose, tiek viešosiose erdvėse siekiant užkirsti kelią žalingam elgesiui, nusikaltimams bei kitokiems visuomenės ramybės trikdžiams. Tačiau

⁶⁸ Europos Komisija, 2020, p. 11–12.

veido atpažinimo technologijų naudojimas darant vaizdo įrašus gali salygoti masinį gyventojų stebėjimą ir žmonės nebegalės būti neatpažinti viešose vietovėse. Veido atpažinimas realiuoju laiku (jei apie tai asmenys žino) gali atgrasytį žmones ne tik lankyti vietovėse, kur yra naudojamos šios technologijos, bet ir įgyvendinti savo konstitucijų garantuojančias teises, tokias, kaip susirinkimų laisvę ir pan.⁶⁹ Tačiau įmanoma ir labai tikėtina, kad žmonės net nežino, kad yra stebimi, ir taip pat gali nežinoti, kad yra stebimi vaizdo kameromis, kurios vykdo veido atpažinimą realiuoju laiku. Taigi, šiuo atžvilgiu svarbi ne tik asmenų baimė, jog jie bus atpažinti ar sekami ten, kur, jų žiniomis, yra įdiegtos pažangios veido atpažinimą įgalinančios vaizdo kameros, bet ir baimė, jog jie gali nežinoti, kur tokios kameros yra naudojamos (pavyzdžiui, Honkonge vykstančiuose protestuose Kinijos valdžia naudojo pažangias veido atpažinimo technologijas, leidžiančias veidus atpažinti net tuo atveju, kai jie yra slepiami⁷⁰), arba baimė, kad, nufilmavus įprasta vaizdo kamera, asmenų duomenys bus apdoroti veido atpažinimo technologijomis ir bus sužinota jų tapatybė.

2.3. Demografinis taikymas ir profiliavimas

Su diskriminacija tiesiogiai susijusi dirbtinio intelekto naudojimo grėsmė yra demografinis taikymas (angl. *demographic targeting*), t. y. kai pasitelkus dirbtinį intelektą siekiama išskirti tam tikrais bruožais apibūdinamą grupę asmenų. Kitaip tariant, remiantis veido, kūno sudėjimo, akies rainelės, balso ar kitais duomenimis sukuriami asmenų demografiniai ir biometriniai profiliai. Nepaisant to, kad tokia informacija gali ir neatskleisti asmens tapatybės, tačiau ji nurodo konkrečią reikiama grupę, kuriai asmuo priskiriamas. Toks demografinis taikymas gali būti naudojamas labai įvairiais tikslais – pavyzdžiui, teisėsaugoje, nustatant galimų nusikaltėlių profilį, ar rinkodaroe, kai taikomasi į konkretias grupes asmenų, kuriems labiausiai norėtusi įsigyti tam tikrą prekę ar paslaugą. Be tokio pobūdžio demografinio „ženklinimo“, naudojamas ir socialinis „ženklinimas“ – pvz., išskiriami homoseksualūs asmenys, tam tikrų ideo-

⁶⁹ Learned-Miller, E., Ordóñez, V., Morgenstern, J., Buolamwini, J. *Facial Recognition Technologies in the Wild: A Call for a Federal Office*, p. 8. Prieiga per internetą: <https://www.semanticscholar.org/paper/FACIAL-RECOGNITION-TECHNOLOGIES-IN-THE-WILD%3A-A-CALL-Learned-Miller-Ordonez/0e637f1cb06f7dd58ed8ad2038fb7bae1e7b45c2>.

⁷⁰ Pvz., žr. In Hong Kong Protests, Faces Become Weapons. *The New York Times*. Prieiga per internetą: <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>, Doffman, Z. Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine. *Forbes*. Prieiga per internetą: <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/?sh=302bee6442b7>.

loginių pažiūrų asmenys ir t. t. Šitoks ženklinimas yra pavojingas tuo, kad asmenys pagal tam tikrą savybę yra priskiriami konkrečiai grupei, kurios atžvilgiu taikomos tos grupės asmenims priskiriamos ir kitos savybės, kurios konkrečiam asmeniui gali būti ir neteisingos (pvz., jei asmuo pensininkas, vadinasi, jis nepasiturintis)⁷¹.

Taigi, naudojant dirbtinį intelektą, paprastai daromi objektų bei reiškinijų subendrinimai. Terminas „subendrinimas“ paprastai suprantamas kaip bet koks platus pobūdžio teiginys apie žmonių grupę ar daiktus – fakto apie kai kuriuos atvejus paverčias faktu apie visus atvejus arba teiginio, kuris kartais gali būti teisingas, pavertimus teiginį, kuris visada teisingas. Mašininių mokymosi kontekste terminas „subendrinimas“ reiškia dirbtinio intelekto modelio gebėjimą teisingai prognozuoti naujus, anksčiau nematytais duomenis, o ne duomenis, naudojamus modeliui mokyti. Mokantis prižiūrint ir neprižiūrint, naujų žinių išmokstama remiantis anksčiau surinktais duomenimis ir šios naujos įžvalgos taikomos prognozuojant. Stiprinant mokymąsi, mašinai leidžiamą mokytis iš savo klaidų, o mokymasis pritaikomas naujose situacijose. Dėl savo potencialiai žmogaus galimybes viršijančių gebėjimų konkrečiose srityse mašininio mokymosi sistemos gali sudaryti įspūdį, kad jos yra protingesnės už žmones ir neklystančios. Tačiau svarbu pabrėžti, kad kaip ir bet kokios formos žmonių ar kompiuterių atlankoje analizėje koreliacija nereiškia priežastinio ryšio, o numatymas nėra tikrumas. Išmokę kompiuteriai gali beveik akimirksniu prognozuoti, bet šias prognozes reikia patikrinti. Nors algoritmai gali atskleisti ryšius tarp įvairių duomenų, labai svarbu patikrinti, ar tie ryšiai yra prasmingi⁷².

2.4. Manipuliacijų rizikos

Kuo daugiau turima duomenų apie konkretų asmenį, tuo daugiau atsiranda galimybų daryti įtaką jo elgesiui ar pasirinkimams. Dirbtinio intelekto algoritmai šiandien naudojami siekiant sukoncretinti interneto erdvėje atsirandančias individualizuotas rekomendacijas – konkrečiam asmeniui siūlomos jam pritaikytos reklamos, pritaikyto turinio tekstai ir t. t.

Šalia konkrečiam asmeniui teikiamų individualizuotų rekomendacijų, tokios sistemos gali sukelti ir grėsmiu, kai žmogus įspraudžiamas į „informacinę burbulą“, kuris nulemia asmens elgesio kaitą, pavyzdžiui, pradeda daugiau pirkti tam tikrų prekių, skaityti tam tikro turinio naujienas ir keisti savo požiūrį į politinius reiškinius, arba

⁷¹ Learned-Miller et al., p. 8.

⁷² OECD, p. 66–67.

net privedti prie priklausomybių ar psichikos sveikatos problemų⁷³. Nors psichikos sveikatos srityje dirbtinis intelektas gali būti naudojamas ir labai teigiamą prasme (pvz., gydant psichikos sutrikimus ar mokant kalbę), yra daug būdų, kai dirbtiniu intelektu piktnaudžiaujama siekiant gauti naudos jo naudotojui galutinių vartotojų sąskaita. Pavyzdžiu, į socialines medijas įdiegtas turinys gali stimuliuoti priklausomybes trikdydamas dopamino lygi žmogaus smegenyse. Tiesa, šiuo atveju „kaltas“ yra ne pats dirbtinis intelektas, bet jo naudojimo kontekstas ir turinys. Manipuliavimas naudojant dirbtinį intelektą yra labai aktualus vaizdo žaidimuose, tačiau taip pat būdingas ir naujienų sklaidai bei filmams, taip pat pranešama apie galimas manipuliacijas transliuojant muzikos kūrinius. Žaisdamas vaizdo žaidimus, asmuo susitapatinė su žaidėju, ir šitaip dirbtinio intelekto naudojimas gali paskatinti asmens priklausomybes tiek nuolat žaisti žaidimus, tiek ir keisti savo elgesį pagal žaidimo aplinką ir realiame gyvenime – o tai gali turėti įvairių neigiamų pasekmių, išskaitant asmeninį, šeimos, profesinį gyvenimą⁷⁴.

2.5. Sprendimų nepaaiškinamumas

Kai valdžios institucijos ar teismai priima sprendimus, jie privalo nurodyti šių sprendimų pagrindimą. Lygiai taip pat, kai tam tikrus sprendimus priima dirbtinis intelektas, iškyla poreikis žinoti, kokiais argumentais ir dėl kokių priežasčių buvo priimtas vienoks ar kitoks sprendimas. Tačiau mašininio ir giliojo mokymosi technologijos nesudaro galimybės žmogui suprasti dirbtinio intelekto veikimo, kadangi jis pats suformuoja tam tikras taisykles iš istoriškai turimų duomenų, ir pateikia sprendimus.

Kai kurie autorai teigia, jog dirbtinio intelekto priimamiems sprendimams turėtų būti taikomas Bendrojo duomenų apsaugos reglamento 15 straipsnio 1 dalies h punktas, pagal kurį tais atvejais, kai yra priimami automatizuoti sprendimai, išskaitant profiliavimą, reikia pateikti prasmingą informaciją apie loginį sprendimo pagrindimą duomenų subjektui. Kylo diskusijų dėl to, ką šiame kontekste reiškia „loginis“ ir kokia informacija būtų „prasminga“ duomenų subjektui. Vyksta akademinė diskusija, ar apskritai yra įmanomas mašininio mokymosi metodu priimto sprendimo pagrįstumo

⁷³ Riehm, K. E., Feder, K. A., Tormohlen, K. N. et al. Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth. *Jama Psychiatry*, 2019, 76(12), p. 1266–1273; Hökby, S., Hadlaczky, G., Westerlund, J., Wasserman, D., Balazs, J., Germanavicius, A., Machín, N., Meszaros, G., Sarchiapone, M., Värnik, A., Varnik, P., Westerlund, M., Carli, V. Are Mental Health Effects of Internet Use Attributable to the Web-Based Content or Perceived Consequences of Usage? A Longitudinal Study of European Adolescents, *JMIR Ment Health*, 2016, No 3(3), p. 31.

⁷⁴ OECD, p. 44.

paaškinimas⁷⁵. Daugiausia nesutarimų kyla dėl to, ar pagal šią nuostatą reikalaujama paaškinti sistemos funkcionalumą – logiką, veikimo eiliškumą, numatomas pasekmės ir bendrą automatizuoto sprendimų priėmimo sistemos apibūdinimą, t. y. sistemos reikalavimų specifikacijas, sprendimų priėmimo medžius, modelius, kriterijus ir klasifikacijų struktūrą, ar konkretaus sprendimo pagrindimą, priežastis, individualias aplinkybes, t. y. aplinkybių pasvērimą, konkrečiam sprendimui taikytas specialias sąlygas ir pan.⁷⁶.

2.6. Asmens orumo pažeidimo rizika

Galimas asmens orumo pažeidimas daugiausia susijęs su asmens atpažinimo technologijų naudojimu. Pirmiausia, atsakant į klausimą, ar, pavyzdžiu, vaizdo stebėjimo kamerų naudojimas pažeidžia asmens orumą, reikia įvertinti, ar jis apriboja asmens galimybes gyventi oriai ir nevaržomai. Ypač tai aktualu kalbant apie realiuoju laiku veikiančias veido atpažinimo priemones, kurios nuolat stebi žmones realiuoju laiku, ir šie stebimi asmenys nežino, kad yra stebimi⁷⁷. Taip pat svarbu, kokia yra vaizdo technologijos naudojama vaizdo rezoliucija, kiek laiko duomenys bus saugomi, kas prie jų turės prieigą ir su kokiais kitais duomenimis jie bus susieti. Kitaip tariant, jei vaizdo stebėjimas ir asmenų atpažinimas kad ir realiuoju laiku vykdomas taip, kad prieigą prie duomenų turi tik įgaliotas asmuo (arba duomenys néra niekur įrašomi), ir duomenys yra ištrinami praėjus kelioms minutėms bei nesusiejami su jokiomis kitomis duomenų bazėmis, kuriose kaupiami duomenys apie tą patį žmogų, privatumo pažeidimas bus minimalus. Tačiau jei vaizdo duomenys yra perduodami į kitas sistemas, kur kaupiama informacija apie asmenį, pavyzdžiu, galima nustatyti, kur jis turėtų būti tuo metu, kai buvo užfiksotas konkrečioje vietoje, kiek dažnai jis ten lankosi, kur fiksotas jo automobilis, kada ir kokiomis sumomis atskaito už kokias prekes ir paslaugas ir t. t. – visas asmens privatus gyvenimas tampa žinomas apibrėžtam ar neapibrėžtam ratui asmenų.

⁷⁵ Goldenein, J. Algorithmic Transparency and Decision-Making Accountability: Thoughts for buying machine learning algorithms. In: Office of the Victorian Information Commissioner (ed). *Closer to the Machine: Technical, Social, and Legal aspects of AI*, 2019, p. 56. Prieiga per internetą: <https://ssrn.com/abstract=3445873>.

⁷⁶ Wachter, S., Mittelstadt, B., Floridi, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 2017, Vol. 7, No. 2, p. 76.

⁷⁷ Montag, L., Mcleod, R., Lara Mets, L., Gauld, M., Rodger, F., Pełka, M. *The Rise and Rise of Biometric Mass Surveillance in EU*, p. 39. Prieiga per internetą: https://edri.org/wp-content/uploads/2021/07/The-Rise-and-Rise-of-Biometric-Mass-Surveillance-in-the-EU_Dutch-Summary.pdf.

2.7. Proporcingumo principio pažeidimai

Anksčiau pateiktas pavyzdys susijęs su dirbtinio intelekto naudojimo proporcingumo užtikrinimo poreikiu, kad nebūtų pažeistos žmogaus teisės. Jungtinė Tautų vyriausasis žmogaus teisių komisaras 2018 metais paskelbė: „Masinių biometrinį duomenų bazės kūrimas kelia didelį susirūpinimą dėl žmogaus teisių. Tokie duomenys yra ypač neviešintini, nes jie iš esmės yra neatsiejamai susiję su konkrečiu asmeniu ir jo gyvenimu ir tuo gali būti rimtais piktnaudžiaujama. Pavyzdžiui, tapatybės vagystė naudojantis biometriniais duomenimis yra labai sunkiai ištaisoma ir gali rimtais paveikti asmens teises. Be to, biometriniai duomenys gali būti naudojami kitais tikslais nei tie, kuriais jie buvo surinkti, išskaitant neteisėtą asmenų sekimą ir stebėjimą. Atsižvelgiant į šią riziką, ypatingas dėmesys turėtų būti skiriamas būtinumo ir proporcingumo klausimams renkant biometrinius duomenis.“⁷⁸

2.8. Techninės ir saugumo rizikos

Dirbtinio intelekto naudojimas susijęs ir su techninėmis rizikomis, kurios gali būti labai įvairios kilmės ir pobūdžio. Pavyzdžiui, labai svarbu, kad dirbtinio intelekto sistema nedarytų „klaidų“ naudodama biometrinį asmenų atpažinimą, nes tokios klaidos tiesiogiai veda į žmogaus teisių pažeidimą – žmogus gali būti apkaltintas dalykais, su kuriais visiškai nebuvo susijęs. Dėl to vienas iš svarbiausių dirbtinio intelekto sistemų bruožų yra jų tikslumas, t. y. kad gautas rezultatas būtų kuo tikslesnis⁷⁹. Būtent dėl šios priežasties Europos Sąjungos dirbtinio intelekto akte išyra siūloma svarbiausiai ir labiausiai pažeidžiamų duomenų tvarkymo sistemoms nustatyti sertifikavimo reikalavimus, t. y. siekiama, kad klaidos tikimybė būtų kuo mažesnė, ir srityse, kur gresia žmogaus teisių pažeidimai, būtų naudojamos tik patikimos dirbtinio intelekto sistemos. Pavyzdžiui, veido atpažinimo technologijos skiriasi pagal galimybę nustatyti konkrečius asmenis, ir nėra sistemos, kuri tai gebėtų daryti 100 procentų. Dėl to kiekviena veido atpažinimo sistema turėtų nurodyti savo klaidos tikimybės procentinį dydį, išskaitant atvejus, kada klaidingai nurodoma, jog asmens tapatybė patvirtinta (pvz., sistemoje ieškant Jono, sistema pateikia rezultatą, kuriame atvaizduotas Tomas), ir atvejus, kai neteisingai asmens tapatybė yra nepatvirtinta (pvz., kai sistemai

⁷⁸ OHCHR. The Right to Privacy in the Digital Age. 3 August 2018, A/HRC/39/29. Prieiga per internetą: <https://undocs.org/A/HRC/39/29>, 14 punktas.

⁷⁹ Kak, A. Regulating Biometrics. Global Approaches and Urgent Questions. AI Now Institute, September 1 2020, p. 27. Prieiga per internetą: <https://ainowinstitute.org/regulatingbiometrics.html>.

užduodama ieškoti Jono, ji nurodo, kad sistemoje Jono atvaizdo nėra). Vertinant, kiek aktuali yra klaidos tikimybė, kalbant tiek apie klaidingą patvirtinimą ir klaidingą nepatvirtinimą, labai svarbu yra kontekstai ir situacijos, kur bandoma atpažinti asmenį⁸⁰. Pavyzdžiui, naudojant veido atpažinimą atrakinant mobilujį telefoną, nėra labai blogai, jei kelis kartus telefonas neatpažįsta jo savininko – kur kas būtų blogiau, jei jis svetimą asmenį atpažintų kaip telefono savininką ir jam suteiktų prieigą prie telefono duomenų. Tačiau kalbant, pavyzdžiui, apie nusikaltėlių sulaikymą, galima turėti omenyje, kad gali būti sulaikyti keli asmenys, ir reikės atlkti išsamesnį tapatybės patikrinimą ir aplinkybių tyrimą, nei neatpažinti né vieno asmens, ypač jei padarytas rimtas nusikaltimas. Tik, kaip buvo minėta, yra labai svarbu atsižvelgti į tai, kad veido atpažinimo klaidos galimybė egzistuoja visada.

Atsižvelgiant į tai, kad dirbtinis intelektas naudoja labai daug duomenų, yra didelė rizika, kad vienu pažeidimu gali būti neteisėtai nutekinta labai daug asmens duomenų. Pavyzdžiui, teisėsaugos srityje dirbtinis intelektas yra labai plačiai naudojamas. Kaip nurodoma EBPO 2019 metais užsakytoje studijoje, daugelio šalių vyriausybės patiria vis daugiau kibernetinio saugumo incidentų, susijusių su didelėmis duomenų bazėmis. Pavyzdžiui, JAV personalo valdymo biuras (angl. *US Office of Personnel Management* (OPM)) nukentėjo nuo kibernetinės atakos, kai buvo nutekinta daugiau nei 21,5 mln. įrašų, išskaitant saugos patikrinimo pagrindinę informaciją, bei 5,6 mln. darbuotojų pirštų atspaudų informaciją⁸¹. Dėl to visos valstybės institucijos ir privatūs subjektai, kurie saugo asmens duomenis, privalo užtikrinti jų saugumą tiek viduje, tiek nuo galimų išorės pasikėsinimų. Ypač svarbu yra užtikrinti biometriinių duomenų saugumą, kadangi biometriniai duomenys yra unikalūs ir negali būti pakeičiami⁸².

Kaip matyti, dirbtinio intelekto naudojimas turi ir šalutinį poveikį – kelia įvairaus pobūdžio ir įvairios prigimties grēsmių tiek tam tikroms visuomenės grupėms, tiek individualiems asmenims. Šios studijos dalies tikslas buvo supažindinti su dirbtinio intelekto keliamų grēsmių bendra situacija, atskirai neaptariant dirbtinio intelekto kūrimo ir naudojimo poveikio asmens privatumui ir duomenų apsaugai. Šie dirbtinio intelekto naudojimo keliamų grēsmių aspektai bus analizuojami atskirame šios studijos skyriuje, prieš tai išanalizavus privatumo ir duomenų, išskaitant biometrinius duomenis, teisinės apsaugos ribas. Tačiau kaip bus matyti, teisės į privatumą ir teisės į asmens duomenų apsaugą užtikrinimas yra susijęs ir su tinkamu aukščiau minėtų dirbtinio intelekto naudojimo rizikų suvaldymu.

⁸⁰ Lynch, J. Face Off. Law Enforcement Use of Face Recognition Technology. *Electronic Frontier Foundation*, 2019, p. 6. Prieiga per internetą: <https://www.eff.org/wp/face-off>.

⁸¹ OECD, p. 81.

⁸² Lynch, p. 11.

3. PRIVATUMO IR ASMENS DUOMENŲ SAMPRATA DIRBTINIO INTELEKTO KONTEKSTE

3.1. Privatumo ir asmens duomenų samprata ir teisinis reguliavimas Europos Sajungoje

Kai kurių mokslininkų (pvz., Karnegio Melono universiteto mokslininko Alessandro Aquisti⁸³) teigimu, sudėtinga spręsti privatumo apsaugos klausimą dėl to, kad privatumą kiekvienas asmuo supranta skirtingai, ir požiūris į tai, kas yra privatu, skiriasi nuo pozicijos, kad privatumo užtikrinimas visiems asmenims yra teisė ir pareiga, iki pozicijos, kad tie, kurie reikalauja privatumo, greičiausiai nori kažką nuslėpti. Ir kadangi sunku apibrėžti, kas yra privatumas, taip pat sunku nustatyti, kada privumas buvo pažeistas. Praktikoje vieni asmenys nekreipia dėmesio į privatumo apsaugos taisykles ir sąmoningai ar nesąmoningai patys nesisaugo nuo kitų asmenų kišimosi į jų privatų gyvenimą ar į tokį kišimąsi nereaguoją, duoda sutikimus prieiti prie asmeninių duomenų nesigilindami, kuo tai gali grësti, tuo pat metu kiti labai atidžiai stebi, kad niekas neturėtų prieigos prie asmeninių, šeimos, medicininių duomenų ar kitos privačios informacijos. Taip pat galima pastebeti, kad visuomenė keičiasi, ypač atsiradus socialiniams tinklams, kur asmenys patys dalinasi privačia informacija su neribotu ratu nepažįstamų asmenų, tai keičia požiūri į privatumą. Ši požiūri taip pat keičia ir technologijų plėtra, kai, norint turėti daugiau patogumo, tenka paaukoti asmeninius duomenis (pavyzdžiu, veido atpažinimas ar pirštų atspaudai naudojami atrakinčių kompiuterių ar telefoną, taip pat patekti į patalpas). P. Danielsono teigimu, riba tarp toleruotino elgesio ir privatumo pažeidimo priklauso ir nuo kultūrinų aspektų, ir nuo technologijų pažangos⁸⁴. Demokratinėse valstybėse paprastai laikoma, kad jei asmuo yra viešoje vietoje, jam neužtikrinama teisė į privatumą (t. y. jis gali būti fotografuojamas ir filmuojamas). Tačiau jei naudojamos pažangios technologijos (galima vaizdą išdidinti daug kartų gera kokybe, automatiškai kontroliuoti filmavimą, filmuo-

⁸³ Acquisti, A. Privacy and security of personal information: Economic incentives and technological solutions. In: Camp, J., Lewis, R. (eds.). *The Economics of Information Security*. Kluwer, Dordrecht, 2004.

⁸⁴ Danielson, P. Video surveillance for the rest of us: Proliferation, privacy, and ethics education. *International Symposium on Technology and Society*, 6–8 June 2002, p. 162–167.

ti nepertraukiamai, naudoti nakties matymo režimą, taikyti įvairius filtrus ir analinius įrankius, ilgai saugoti filmuotą medžiagą) ir ypač jei vaizdo įrašas daromas ne vienoje vietoje, arba jis sujungiamas su kitokio pobūdžio duomenimis apie tą patį asmenį (telefono GPS signalas, pokalbių ar žinučių telefonu adresatai, interneto ir socialinių tinklų naršymo istorija, automobilio numeris, asmens darbovietė, GPS duomenys arba gatvių stebėsenos duomenys, banko ar mokėjimų sąskaitos duomenys ir t. t.), tuomet kyla klausimas, ar tikrai asmens filmavimas viešoje vietoje nėra susijęs su jo privatumo pažeidimu⁸⁵.

Tačiau dėl asmens duomenų apibréžimo yra aiškiau, kadangi ši sąvoka yra apibréžta Bendrajame asmens duomenų apsaugos reglamente ir Duomenų apsaugos teisėsaugos srityje direktyvoje. Remiantis šiais dokumentais asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybę nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti visų pirmą pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vienos duomenis ir interneto identifikatorių arba pagal vieną ar keliis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius⁸⁶. Kaip bus matyti, specialus ir griežtesnis apsaugos režimas yra taikomas biometriniams asmens duomenims. Pagal minėtus Europos Sąjungos teisės aktus, biometriniai duomenys – tai po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys⁸⁷. Pagal Bendrajį duomenų apsaugos reglamentą (kartu ir Duomenų apsaugos teisėsaugos srityje direktyvą), biometriniai duomenys yra tik tie duomenys, kurie specialiai techniškai apdoroti. Taigi tokie asmens duomenys, kaip veido atvaizdas, balsas, eisena bei kiti bruožai, kol nėra apdoroti specialiomis priemonėmis, yra laikomi „paprastais asmens duomenimis“ ir jiems netaikomas biometrinių duomenų apsaugos režimas.

⁸⁵ Li S. Z., Jain A. K. *Handbook of Face Recognition*. Springer, 2011, p. 672.

⁸⁶ Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokų duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – Bendrasis duomenų apsaugos reglamentas, BDAR), OL L 119/I, 4 straipsnis 1 punktas; Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamomo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokų duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR (toliau – Teisėsaugos direktyva), OL L 119/89, 3 straipsnio 1 dalis.

⁸⁷ BDAR 4 straipsnio 14 punktas, Teisėsaugos direktyvos 3 straipsnio 13 dalis.

Prieiga gerbti privatų gyvenimą ir asmeninių duomenų apsauga Europos Sąjungos pagrindinių teisių chartijoje reguliuojami atskirai (atitinkamai 7 straipsnyje „Teisė į privatų ir šeimos gyvenimą“ numatyta, kad kiekvienas asmuo turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir komunikacijos slaptumas, o 8 straipsnyje „Asmens duomenų apsauga“ nustatyta, kad kiekvienas asmuo turi teisę į savo asmens duomenų apsaugą⁸⁸), o Europos žmogaus teisių konvencijoje (toliau – EŽTK) šios abi teisės numatytos tame pačiame 8 straipsnyje „Teisė į privataus ir šeimos gyvenimo gerbimą“: „Kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas. Valstybės institucijos neturi teisės apriboti naudojimosi šiomis teisėmis, išskyrus įstatymų nustatytus atvejus ir, kai tai būtina demokratinėje visuomenėje valstybės saugumo, visuomenės saugos ar šalies ekonominės gerovės interesams, siekiant užkirsti keilių viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.“⁸⁹

Europos Žmogaus Teisių Teismas (toliau – EŽTT) yra pateikęs išaiškinimų dėl EŽTK 8 straipsnio ir asmenų stebėjimo. Teismas pabrėžė, kad tai, jog valdžios institucijos turi galimybę gauti išsamią asmeninio pobūdžio informaciją apie asmenį su jungdamos duomenis iš įvairių šaltinių, laikytina ypač dideliu kišimusi į asmeninį gyvenimą⁹⁰. Šiame kontekste itin svarbu, kad dirbtinio intelekto technologijos sudaro galimybes susieti asmens duomenis iš įvairių šaltinių ir vienoje vietoje turėti išsamią informaciją apie konkretų asmenį⁹¹.

EŽTT pabrėžia, kad yra labai svarbu užtikrinti, jog asmenys bus informuojami apie duomenų apie juos rinkimą, įskaitant ir stebėjimo kamerų duomenis. *Libertybyloje*⁹² buvo sprendžiamas klausimas dėl telefono pokalbių perėmimo ir vėlesnio filtravimo technologijų naudojimo, kai buvo ieškoma žodžių pagal raktinių žodžių sąrašą, šį procesą kontroliuojant konkretiems valdžios institucijų darbuotojams. Teismas nusprennė, kad pagal tuometinę teisinę reguliaivimą nebuvo pakankamai aišku, kokias teises turi valdžios institucijos apdoroti ir tvarkyti duomenis, gautos perėmus pokalbius

⁸⁸ Europos Sąjungos pagrindinių teisių chartija. OL C 202/389.

⁸⁹ Europos žmogaus teisių konvencija. Prieiga per internetą: https://www.echr.coe.int/documents/convention_lit.pdf.

⁹⁰ Europos Žmogaus Teisių Teismo sprendimas Szabó ir Vissy prieš Vengriją, 70 punktas. Prieiga per internetą: <https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001-160020&filename=CASE%20OF%20SZAB%C3%93%20AND%20VISSY%20v.%20HUNGARY.pdf>.

⁹¹ European Parliament. Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights, p. 38. Prieiga per internetą: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU-\(2020\)656295](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU-(2020)656295).

⁹² Europos Žmogaus Teisių Teismo sprendimas Liberty ir kiti prieš Jungtinę Karalystę. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-1980>.

telefonu, ir dėl to buvo pažeistas EŽTK 8 straipsnio reikalavimas „išskyrus įstatymų nustatytus atvejus“.

Sprendime *Weber ir Saravia prieš Vokietiją* prie būtinų sąlygų, kai gali būti pateisintas kišimasis į asmenų privatų gyvenimą, EŽTT nurodo pranešimą asmenims apie informacijos rinkimą. Tačiau pranešimas nebūtinai turi būti pateikiamas duomenų rinkimo metu, jis gali būti pateiktas ir vėliau, t. y. kai tik jis nebekels grėsmės duomenų rinkimo tikslui pasiekti⁹³.

2020 m. *Gaughran*⁹⁴ prieš Jungtinę Karalystę byloje dėl nuteisto asmens DNR profilio, pirštų atspaudų ir nuotraukos buvo keliamas klausimas, ar buvo teisėta turėti prieigą prie duomenų bazės, kurioje buvo laikomos nuotraukos, turint tikslą naudoti veido atpažinimo technologijas, kai duomenys galėjo būti perkelti į kitą duomenų bazę, kurioje nebuvo galimybės naudoti veido atpažinimo technologiją. Šiame sprendime EŽTT aiškiai atmetė Jungtinės Karalystės vyriausybės argumentą, pagal kurį „kuo daugiau duomenų laikoma, tuo daugiau nusikalstamų veikų yra užkardoma“, pažymėdamas, kad „tokio argumento dėl neriboto duomenų laikymo priėmimas prilygtų pateisiniui laikyti duomenis apie visus šalies gyventojus, išskaitant jų mirusius artimuosius“⁹⁵.

2020 metais Nyderlanduose Hagos apygardos teismas nagrinėjo bylą dėl valdžios institucijų taikomų rizikos reitingų. Sisteminis rizikos indikatorius (SyRI) buvo įrankis, kurį Nyderlandų vyriausybė naudojo kovai su sukčiavimu. Kelios pilietinės visuomenės organizacijos apskundė šio įrankio taikymą. Nyderlandų įstatymų leidėjas apibūdino SyRI kaip techninę infrastruktūrą su galimybe sieti ir analizuoti duomenis turint tikslą sugeneruoti rizikos ataskaitas. Remiantis tokią ataskaitų rezultatais būtų aišku, kad konkretų asmenį yra verta tirti dėl galimo sukčiavimo, piktnaudžiavimo padėtimi ar teisės aktų nesilaikymo. Šį instrumentą buvo galima naudoti, kai to praše tam tikros viešosios valdžios institucijos ar valdžios funkcijas vykdančios įstaigos, tokios, kaip savivaldybių institucijos, Nyderlandų mokesčių ir muitinės administracija, Socialinių reikalų ir įdarbinimo inspekcija, Imigracijos ir natūralizacijos tarnyba. SyRI naudojami duomenys apėmė duomenis apie darbą, išsilavinimą, mokesčių mokėjimą, turtą, gyvenamają vietą, taikytas administracines nuobaudas, pilietinę padėtį, socialines pašalpas ar pagrindus dėl atsisakymo skirti pašalpas, pensijas, skolas, taikytas reintegracijos priemones bei kai kuriuos sveikatos apsaugos draudimo duomenis. Savo sprendime Hagos apygardos teismas pažymėjo, kad skaitmeninės sėsajos tarp duo-

⁹³ Europos Žmogaus Teisių Teismo sprendimas *Weber ir Saravia prieš Vokietiją*, 135 punktas. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=001-76586>.

⁹⁴ Europos Žmogaus Teisių Teismo sprendimas *Gaughran prieš Jungtinę Karalystę*. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-12731>.

⁹⁵ *Gaughran* sprendimo 89 punktas.

menų laikmenų ir algoritmų taikymas sudaro galimybę valdžios institucijoms keistis duomenimis, kurie yra reikalingi vykdyti šioms institucijoms įstatymais pavestas funkcijas – užkirsti kelią sukčiavimui. Teismas nusprendė, kad tokią naujų technologinių galimybių naudojimas užkardant sukčiavimą yra leistinas. Tačiau kartu teismas pažymėjo, kad naujų technologijų plėtra taip pat reiškia, kad teisė į asmens duomenų apsaugą kartu didėja ir iجاuna vis didesnę svarbą. Naudojant šias technologijas gali stipriai išaugti kišimasis į asmenų privatų gyvenimą, tačiau asmenims yra sudėtinga apginti savo teises, dėl to vyriausybei ir viešosios valdžios institucijoms tenka „ypatinga atsakomybė“ taikant tokias priemones kaip SyRI. Šioje byloje atlikęs išsamų vertinimą teismas nusprendė, kad SyRI instrumento reguliavimas buvo nepakankamas ir neatitinko EŽTK 8 straipsnyje keliamų reikalavimų, susijusių su pareiga gerbti privatų gyvenimą, kadangi pagal šį straipsnį numatyta išimtis gali būti taikoma tik kai tai būtina demokratinėje visuomenėje, t. y. tik tais atvejais, kai tokia priemonė yra būtina ir proporinga siekiama tikslui. Šiame kontekste teismas pažymėjo, kad, išnagrinėjus SyRI sistemos veikimo tikslą ir pagrindus remiantis Europos Sąjungos pagrindinių teisių chartija ir Bendrojo asmens duomenų reglamento nuostatomis, ypač atsižvelgiant į skaidrumo, tikslų ribojimo ir duomenų mažinimo principus, nustatyta, kad sistema buvo nepakankamai skaidri ir patikima⁹⁶. Žmogaus teisių gynėjai labai sveikino šį sprendimą, kadangi juo buvo sustabdyta viešosios valdžios iniciuota dirbtinio intelekto priemonėmis diegiama kampanija „sustabdyk sukčiavimą jam dar neprasidejus“, kai buvo siekiama stebeti pašalpų prašytojus, išskaitant asmenis labai pažeidžiamose situacijose⁹⁷.

Kaip nurodoma Pagrindinių teisių agentūros dokumente „Veido atpažinimo technologijos: pagrindinių teisių aspektai teisėsaugos institucijų veikloje“⁹⁸, „privataus gyvenimo“ apibrėžimas yra platus, ir niekur nėra pateiktas jo baigtinis sąrašas. Ši sąvoka apima asmens fizinio ir psichologinio gyvenimo aspektus ir gali atspindėti įvairius asmens fizinius bei socialinės tapatybės bruožus. „Privataus gyvenimo“ apibrėžimas taip pat kai kuriais atvejais, kaip išaiškino EŽTT sprendime *López Ribalda ir kiti prieš Ispaniją*, gali apimti ir asmens santykį su kitais asmenimis sričių⁹⁹. Kituose kontek-

⁹⁶ Judgment of The Hague District Court of 5 February 2020, case number C/09/550982, ECLI:NL:RBDHA:2020:865.

⁹⁷ Privacy International, The SyRI case: a landmark ruling for benefits claimants around the world. Prieiga per internetą: <https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world>.

⁹⁸ European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement, p. 23. Prieiga per internetą: <https://fra.europa.eu/en-publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>.

⁹⁹ Europos Žmogaus Teisių Teismo sprendimas *López Ribalda ir kiti prieš Ispaniją*, 87 punktas. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-12630>.

tuose EŽTT vartoja „pagrįstų privatumo lūkesčių“ sąvoką referuodamas į tai, kiek žmonės gali tikėtis privatumo viešose erdvėse, kur néra stebėjimo kamero – tai yra vienas iš veiksnių, nors nebūtinai lemiamas, sprendžiant dėl teisės į privatų gyvenimą pažeidimo. Tačiau vien tik faktas, kad viešose vietose yra įrengtos vaizdo stebėjimo kameros, automatiškai nereiškia, kad asmens teisė į privatumą yra pažeista. Panašiai teigia ir Jungtinių Tautų ekspertai – tai, kad žmonės susirenka viešoje vietoje, nereiškia, kad jų privatumas bus pažeistas, jei bus filksuojamas vaizdas stebėjimo kameros¹⁰⁰. Kur kas didesnę grėsmę asmens privatumui ir asmens duomenų apsaugai kelia vaizdo duomenų apdorojimas naudojant veido atpažinimo technologijas. Nors teisė į privataus gyvenimo apsaugą ir teisė į privatumą néra absoliučios teisės, t. y. jos gali būti apribotos, tačiau bet koks ribojimas turi būti tinkamai pateisinamas¹⁰¹.

Kaip nurodo Pagrindinių teisių agentūra, veido atpažinimo technologijų naudojimas realiuoju laiku yra susijęs su biometriniių duomenų, gautų viešose vietose, apdorojimu, siekiant nustatyti asmens tapatybę (1:n identifikavimas), ir potencialiu tokiu duomenų saugojimu. Taigi, tiek pirminis veido atvaizdų apdorojimas naudojant veido atpažinimo technologijas, tiek ir vaizdo medžiagos ar apdorotų biometriniių duomenų saugojimas ir jų vėlesnis palyginimas su kitais duomenimis yra susiję su kišimusi į asmens privatų gyvenimą ir asmens duomenų apsaugos ribojimu¹⁰². Kaip buvo minėta, tokis specialia technologija apdorotų asmens duomenų tvarkymas yra laikomas biometriniių duomenų tvarkymu, ir dėl to taikomi griežtesni duomenų apsaugos reikalavimai. Bet kuriuo atveju asmens duomenų tvarkymo veiksmai turi būti pagrįsti ir proporcingi, tam turi būti aiškus teisinis pagrindas ir teisėtas tikslas.

Šalia pagrindinių teisių saugiklių ir pagrindinių asmens duomenų apsaugos reikalavimų, kylančių iš Europos Sąjungos pagrindinių teisių chartijos bei Europos Sąjungos Teisingumo Teismo išaiškinimų bei EŽTK ir EŽTT išaiškinimų, Europos Sąjungoje taikomos papildomos apsaugos taisyklės dėl taikomų priemonių būtinumo ir proporcingumo testo. Taip pat, kalbant apie biometriniių duomenų tvarkymą, remiantis Bendrojo asmens duomenų apsaugos reglamento 9 straipsnio 2 dalies g punktu, biometrinius duomenis galima tvarkyti tik kai tvarkyti duomenis būtina dėl svarbaus viešojo interesu priežasčių, remiantis Sąjungos arba valstybės narės teise, kurie turi

¹⁰⁰ UN Human Rights Committee, draft General Comment No. 37 [Article 21: right of peaceful assembly], draft prepared by the Rapporteur, Christof Heyns, 2019, 69 punktas. Prieiga per internetą: <https://www.ohchr.org/en/calls-for-input/call-comment-no-37-article-21-international-covenant-civil-and-political-rights>.

¹⁰¹ FRA, Council of Europe and EDPS. *Handbook on European data protection law*. Luxembourg, Publications Office, June 2018, p. 35–52.

¹⁰² Fussey, P., Murray, D. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. University of Essex, Human Rights Centre, July 2019, p. 36.

būti proporcinių tikslui, kurio siekiama, nepažeisti esminių teisės į duomenų apsaugą nuostatų ir kuriuose turi būti numatytos tinkamos ir konkrečios duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės; o teisėsaugos srityje remiantis Duomenų apsaugos teisėsaugos srityje direktyva tvarkyti biometrinius asmens duomenis galima tik tada, jei tai tikrai būtina ir jei taikomos tinkamos duomenų subjekto teisių ir laisvių apsaugos priemonės, ir jeigu tai leidžiamas pagal Sajungos arba valstybės naės teisę; tai reikalinga duomenų subjekto ar kito fizinio asmens gyvybiniams interesams apsaugoti, arba toks tvarkymas susijęs su duomenimis, kuriuos duomenų subjektas yra akivaizdžiai paskelbęs viešai¹⁰³.

Taigi, tvarkant asmens duomenis turint tikslą juos apdoroti specialiomis technologijomis, būtina laikytis teisinių reikalavimų. Remiantis pagrindiniais asmens duomenų apsaugos principais, asmens duomenų tvarkymas turi būti 1) teisėtas ir skaidrus; 2) vykdomas turint konkretų, aiškų ir teisėtą tikslą (aiškiai apibrėžta valstybės naės ar Europos Sajungos teisės aktuose) ir 3) tenkinti duomenų mažinimo, duomenų tikslumo, saugojimo ribojimo, duomenų apsaugos ir atskaitingumo reikalavimus¹⁰⁴.

3.2. Privatumo ir asmens duomenų apsaugos reguliavimas ir praktika Lietuvoje

Lietuvos Respublikos Konstitucijoje (toliau – Konstitucija) numatyta, kad žmogaus privatus gyvenimas neliečiamas; asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami; informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą; įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą¹⁰⁵. Nors Lietuvoje nėraatskiro įstatymo, kuriuo būtų reguliuojama asmens privatumo apsauga, Lietuvos Respublikos Konstitucinis Teismas (toliau – Konstitucinis Teismas), nagrinédamas konstitucines bylas, pateiké kelis oficialius šios nuostatos išaiškinimus. Taip pat teisės į privatumą pagrindai reguliuojami Lietuvos Respublikos civiliniame kodekse (toliau ir – Civilinis kodeksas)¹⁰⁶.

Pirma, pagal Konstituciją, privatus žmogaus gyvenimas – tai individu asmeninis gyvenimas: gyvenimo būdas, šeimyninė padėtis, gyvenamoji aplinka, santykiai su ki-

¹⁰³ Teisėsaugos direktyva.

¹⁰⁴ Teisėsaugos direktyvos 4 straipsnis, BDAR 5 straipsnis.

¹⁰⁵ Lietuvos Respublikos Konstitucijos (Žin., 1992, Nr. 33-1014) 22 straipsnis.

¹⁰⁶ Lietuvos Respublikos civilinis kodeksas (Žin., 2000, Nr. 74-2262).

tais asmenimis, individu pažiūros, įsitikinimai, įpročiai, jo fizinė bei psichinė būklė, sveikata, garbė, orumas ir kt. Konstitucijos normose įtvirtintas žmogaus privataus gyvenimo neliečiamumas suponuoja asmens teisę į privatumą. Žmogaus teisė į privatumą apima asmeninio, šeimos ir namų gyvenimo, garbės ir reputacijos neliečiamumą, asmens fizinę ir psichinę neliečiamybę, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidentialią informaciją ir kt.¹⁰⁷ Be to, pasak Konstitucinio Teismo, asmens privatus gyvenimas yra plati kategorija, kurią sunku tiksliai visiems atvejams apibrėžti. Konstitucijos 22 straipsnyje įtvirtinta asmens teisė į jo privataus gyvenimo gerbimą ir šios teisės apsauga aiškintina plečiamai, remiantis dinaminiu žmogaus teisių aiškinimo principu, atsižvelgiant *inter alia* į visuomenės raidą, mokslo ir technologijų pažangą, suteikiančią vis daugiau galimybių kištis į asmens privatų gyvenimą, kaip antai nusikalstamų veikų prevencijos ar kitais viešosios tvarkos apsaugos tikslais renkant, kaupiant, naudojant ir saugant ne tik asmens pirštų atspaudų, jo balso, bet ir asmens laštelį ar DNR mėginių pavyzdžius, technikos priemonėmis masiškai stebint ir sekant asmenų naudojamas elektronines erdves, *inter alia* su globalinės padėties nustatymo sistema (GPS) nustatant asmenų buvimo vietą¹⁰⁸.

Konstitucinis Teismas pabrėžia, kad Konstitucijos 22 straipsnio 3 dalies nuostata „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“, taip pat 4 dalies nuostata „įstatymas ir teismas sau-go, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, késinimosi į jo garbę ir orumą“ yra vienos svarbiausių asmens privataus gyvenimo neliečiamybės garantijų. Jomis asmens privatus gyvenimas saugomas nuo valstybės, kitų institucijų, jų pareigūnų, kitų asmenų neteisėto kišimosi¹⁰⁹.

Tačiau kartu atkrepiamasi dėmesys į tai, kad privataus gyvenimo teisinė samprata siejama su asmens būsena, kai asmuo gali tikėtis privatumo, su jo teisėtais privataus gyvenimo lūkesčiais¹¹⁰. Vadinas, tam, kad nebūtų privatumo pažeidimo, asmuo turi žinoti, kad jo atžvilgiu yra taikomos stebėjimo ar duomenų rinkimo priemonės. Ir tuo atveju, jei asmuo yra viešoje vietoje, greičiausiai negalėtų tikėtis, kad tikrai nepaklius į daromą vaizdo įrašą, jei saugumo tikslais viešoje vietoje yra įrengta stebėjimo kamera, ir ypač tais atvejais, jeigu yra įrengti įspėjamieji ženklai. Taigi tokiu atveju reikalavimas aiškiai pagrįsti tokios stebėjimo kameros įrengimą įstatymu nuostatomis užtikrinant duomenų saugumo reikalavimus yra validus, tačiau asmuo greičiausiai nei-

¹⁰⁷ Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d., 2000 m. gegužės 8 d., 2002 m. rugsėjo 19 d., 2002 m. spalio 23 d., 2003 m. kovo 24 d. nutarimai.

¹⁰⁸ Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas.

¹⁰⁹ Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas.

¹¹⁰ Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas.

rodytų, kad tokiam filmavimui yra būtinės teismo leidimas remiantis Konstitucijos 22 straipsniu, nes tai savaimė nebūtų informacijos apie privatų asmens gyvenimą rinkimas. Taip pat Konstitucinis Teismas nurodo, kad esama tokį privataus gyvenimo sričių (pavyzdžiui, intymus gyvenimas), apie kurias informacija be asmens sutikimo apskritai negali būti renkama ir skelbiama, nebent (ir tik tuo mastu, kuriuo) tai pade- da atskleisti to asmens padarytą nusikaltimą¹¹¹.

Konstitucinis Teismas atkreipia dėmesį į tai, kad žmogaus teisę į privatumą nėra absoluti, ir yra pasiakęs apie konkrečius teisės į privatumą ribojimus.

Pagal Konstituciją, riboti konstitucines žmogaus teises ir laisves, tarp jų ir teisę į privatumą, galima, jeigu yra laikomasi šių sąlygų: tai daroma įstatymu; ribojimai yra būtini demokratinėje visuomenėje siekiant apsaugoti kitų asmenų teises bei laisves ir Konstitucijoje įtvirtintas vertybes, taip pat konstituciškai svarbius tikslus; ribojimais nėra paneigiamos teisių ir laisvių prigimtis bei jų esmė; yra laikomasi konstitucinio proporcingumo principo¹¹².

Be to, asmuo, darydamas nusikalstamas ar kitas priešingas teisei veikas, neturi ir negali tikėtis privatumo. Žmogaus privataus gyvenimo apsaugos ribos baigiasi tada, kai jis savo veiksmais nusikalstamai ar kitaip neteisėtai pažeidžia teisės saugomus interesus, daro žalą atskiriems asmenims, visuomenei ir valstybei. Taip pat visiško privatumo asmuo negali tikėtis ir tada, kai jis pažeidžia privačios teisės normas, reguliuojančias komercinę ar kitokią privataus pobūdžio paslaptį¹¹³. Tačiau kituose išaiškinimuose Konstitucinis Teismas pabrėžia, kad tokiais atvejais teisės į privatumą ribojimai turi būti būtini ir proporcingi. Pavyzdžiui, dėl organizuoto nusikalstamumo užkardymo Konstitucinis Teismas yra nurodės, kad tam, jog asmuo nepatirtų savvališko ir nepagrįsto teisės į privatumą suvaržymo, prevencinės poveikio priemonės, kuriomis įsiterpiama į žmogaus teisės į privatų gyvenimą įgyvendinimą, gali būti skirtinos tik įstatyme nustatytais pagrindais, laikantis įstatyme nustatytos tvarkos ir numatant asmens teisę paskirtą prevencinę poveikio priemonę apskursti teismui. Tačiau tokias priemones taikančios institucijos kiekvienu atveju turi įvertinti konkrečią situaciją, ištirti visas turinčias reikšmės aplinkybes, išsiaiškinti, ar negalima tą pačią tikslų pasiekti neįsiterpiant į privatų žmogaus, šeimos gyvenimą ir neapribojant žmogaus teisės į privatumą labiau negu būtina minėtam visuomenei reikšmingam ir konstituciškai pagrįstam tikslui pasiekti¹¹⁴.

¹¹¹ Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas.

¹¹² Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugpjūto 19 d., 2002 m. spalio 23 d., 2003 m. kovo 24 d. nutarimai.

¹¹³ Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas.

¹¹⁴ Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas.

Kalbant apie viešuosius asmenis (t. y. politikus, valstybės ir savivaldybių pareigūnus, visuomeninių organizacijų vadovus bei kitus asmenis, jeigu jų veikla turi reikšmės viešiesiems reikalams), Konstitucinis Teismas pabrėžia, kad jų atžvilgiu gali būti taikoma daugiau išimčių iš pareigos saugoti jų privatą gyvenimą – be šių asmenų sutikimo gali būti skelbiama informacija apie jų privatą gyvenimą tokiu mastu, kokiui to asmens asmeninės savybės, elgesys, kitos privataus gyvenimo aplinkybės gali turėti reikšmės viešiesiems reikalams ir dėl to skelbiama informacija turi visuomeninę reikšmę. Tačiau kartu Konstitucinis Teismas pabrėžė, kad įstatymuose turi būti apibrėžti kriterijai, pagal kuriuos tam tikrus asmenis galima priskirti viešiesiems asmenims¹¹⁵.

Dėl žmogaus orumo nepažeidžiamumo Konstitucinis Teismas konstatavo, kad, pagal Konstituciją, žmogaus orumo apsauga neatsiejama nuo jo privataus gyvenimo apsaugos, garantuojamos 22 straipsnio 1 dalyje. Asmens fizinis ir psichinis neliečiamumas sudaro asmens neliečiamumo turinį ir yra apimamas asmens teisės į privatumą. Todėl, kėsinantis į asmens neliečiamumą – jo fizinę ar psichinę neliečiamybę, kartu savavališkai ir neteisėtai kišamasi į jo privatą gyvenimą, taigi kėsinamasis ir į jo garbę ir orumą¹¹⁶.

Tačiau bet kuriuo atveju, pagal Konstituciją, *inter alia* jos 22 straipsnį, asmens privataus gyvenimo gerbimo principas suponuoja pozityvias valstybės pareigas imtis atitinkamų priemonių siekiant užtikrinti asmens teisę į jo asmeninio ir šeimos gyvenimo, taip pat jo garbės ir orumo apsaugą *inter alia* slapta renkant informaciją apie asmenį baudžiamosios justicijos ar kitais teisėtais tikslais, taip pat panaudojant minėtą informaciją įstatymuose nustatytais atvejais ir tvarka¹¹⁷.

Kelios nuostatos dėl asmens privatumo apsaugos numatytos Civiliniame kodekse. Šio kodekso 1.114 straipsnyje nustatyta, kad civilinė teisė saugo asmenines neturtines teises ir vertybes, su kuriomis įstatymai sieja tam tikrų teisinių pasekmių atsiradimą, *inter alia*, vardą, garbę, orumą, žmogaus privatą gyvenimą, dalykinę reputaciją. Kodekso 2.23 straipsnyje įtvirtinta, kad fizinio asmens privatus gyvenimas neliečiamas ir informacija apie asmens privatą gyvenimą gali būti skelbiama tik jo sutikimu. Taip pat nurodoma, kad privataus gyvenimo pažeidimu laikomas neteisėtas jėjimas į asmens gyvenamąsias ir kitokias patalpas, aptvertą privačią teritoriją, neteisėtas asmens stebėjimas, neteisėtas asmens ar jo turto apieškojimas, asmens telefoninių pokalbių susirašinėjimo ar kitokios korespondencijos bei asmeninių užrašų ir informacijos konfidencialumo pažeidimas, duomenų apie asmens sveikatos būklę paskelbimas pažeidžiant įstatymų nustatyta tvarką bei kitokie neteisėti veiksmai. Taip pat draudžiama

¹¹⁵ Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas.

¹¹⁶ Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 19 d. išvada.

¹¹⁷ Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas.

rinkti informaciją apie privatų asmens gyvenimą pažeidžiant įstatymus. Asmuo turi teisę susipažinti su apie jį surinkta informacija, išskyrus įstatymų nustatytas išimtis. Draudžiama skleisti surinktą informaciją apie asmens privatų gyvenimą, nebent, atsižvelgiant į asmens einamas pareigas ar padėtį visuomenėje, tokios informacijos skleidimas atitinka teisę ir pagrįstą visuomenės interesą tokią informaciją žinoti. Taip pat nurodoma, kad apribojimai, susiję su informacijos apie asmenį skelbimu ir rinkimu, netaikomi, kai tai daroma motyvuotu teismo sprendimu.

Civilinis kodeksas reguliuoja teisę į atvaizdą. Kodekso 2.22 straipsnyje nustatyta, kad fizinio asmens nuotrauka (jos dalis), portretas ar kitoks atvaizdas gali būti atgauminami, parduodami, demonstruojami, spausdinami, taip pat pats asmuo gali būti fotografuojamas tik jo sutikimu. Asmens sutikimo nereikia, jeigu šie veiksmai yra susiję su visuomenine asmens veikla, jo tarnybine padėtimi, teisėsaugos institucijų reikalavimu arba jeigu fotografuojama viešoje vietoje. Tačiau asmens nuotraukos (jos dalies), padarytos šiais atvejais, negalima demonstruoti, atgaminti ar parduoti, jeigu tai pažemintų asmens garbę, orumą ar dalykinę reputaciją.

Pažeidus asmens teisę į privatumą ar į atvaizdą, asmuo gali kreiptis į teismą prašydamas atlyginti padarytą turtinę ir neturtinę žalą.

Apibendrinant galima teigti, kad, naudojant dirbtinį intelektą visuomenės gyvenime, svarbu atsižvelgti į šią Konstitucinio Teismo doktriną dėl privataus gyvenimo apsaugos:

- užtikrinant privataus gyvenimo apsaugą būtina atsižvelgti į visuomenės raidą bei mokslo ir technologijų pažangą;
- asmuo turi žinoti (iš anksto ar bent jau *post factum*) apie jo atžvilgiu naudotą asmens duomenų rinkimą;
- taikant bet kokią priemonę, kuria ribojama teisę į privatumą, turi būti įvertinama, ar negalima tų pačių tikslų pasiekti nejisiterpiant į privatų žmogaus, šeimos gyvenimą ir neapribojant žmogaus teisés į privatumą;
- teisę į privatumą apima ir teisę į psichinių neliečiamumą. Vadinas, pasitelkiant dirbtines technologijas kuriamos manipuliacinės priemonės (pvz., skatinimas daugiau pirkti tam tikrų produktų) yra susijusios su teisés į privatumą pažeidimu.

Remiantis Civiliniu kodeksu, neleidžiamas neteisėtas asmens stebėjimas, draudžiama rinkti informaciją apie privatų asmens gyvenimą pažeidžiant įstatymus; leidžiamas asmens fotografavimas viešoje vietoje, tačiau yra nustatyti ribojimai gautų nuotraukų naudojimui.

Atsižvelgiant į tai, kad asmens duomenų apsauga nėra specialiai išskirta teisė Lietuvos Respublikos Konstitucijoje, Konstitucinio Teismo jurisprudencijos šiuo aspektu nėra daug. Tačiau Teismas pažymėjo, kad Konstitucijos 22 straipsnio 3, 4 dalyse

yra įtvirtinta įstatymų leidėjo pareiga informacijos apie privatų asmens gyvenimą rinkimo tvarką nustatyti įstatymu¹¹⁸. Todėl, pagal Konstituciją, *inter alia* jos 22 straipsnį, konstitucinį teisinės valstybės principą, įstatymų leidėjui, jam nustačius valstybės institucijų įgaliojimus įstatymo nustatytais atvejais ir tvarka slapta rinkti informaciją apie asmenis baudžiamosios justicijos ar kitais teisėtais tikslais, kyla pareiga įstatyme nustatyti ir tokios surinktos informacijos panaudojimo atvejus ir sąlygas, *inter alia* įtvirtinti galimybę perduoti šią informaciją naudoti kitoms valstybės institucijoms įstatymuose nustatytais kitais teisėtais tikslais, be kita ko, tarnybinių nusižengimų tyrimui¹¹⁹.

Asmens duomenų tvarkymui Lietuvoje taikomi du pagrindiniai dokumentai – Bendrasis duomenų apsaugos reglamentas ir Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas¹²⁰, kuris iš esmės tiesiogiai atkartoja Duomenų apsaugos teisėsaugos srityje direktyvos nuostatas dėl asmens duomenų ir biometrinės asmens duomenų tvarkymo. Šiuose teisės aktuose išdėstyti su asmens duomenų apsauga susiję reikalavimai, kurių privalo laikytis visi viešojo ir privataus sektoriaus subjektai.

Teismų praktika dėl asmens duomenų pažeidimo atvejais, kurie yra ar gali būti susiję su dirbtinio intelekto naudojimu (pvz., kad vaizdo įrašo medžiaga bus specialiai apdorota siekiant gauti biometrinius duomenis), nėra gausi. Antai 2017 m. byloje dėl daugiabučio namo prieigose vykdomo filmavimo siekiant užtikrinti butų savininkų ir jų turto saugumą, kai tokiam filmavimui prieštaravo keli iš namo bendrasavininkų, Lietuvos Aukščiausiasis Teismas nurodė, kad atsižvelgiant į tai, jog į kameromis filmuojamą vaizdą patenka ir ieškovams priklausantis turtas (butai, kiemas, jėjimo durys, laiptinė), asmenys, gyvenantys name, bei į namą ateinantys pašaliniai asmenys, taip pat tai, kad bendarurčiams priklausantis pastatas ir jo kiemas nėra vieša vieta, o byloje nebuvvo įrodyta, jog kamerų įrengimo tikslas (apsaugoti savo turtą nuo sugadinimo) yra proporcingas siekiui riboti ieškovų privatų gyvenimą, darytina išvada, kad vykdomas vaizdo stebėjimas nors ir teisėtu tikslu, tačiau neatitinka įstatymo 19 straipsnio 1 dalies nuostatų tiek stebimos teritorijos, tiek renkamų vaizdo duomenų apimčių prasme, todėl ieškovų pažeistos asmens duomenų apsaugos teisės yra gintinos¹²¹.

¹¹⁸ Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas.

¹¹⁹ Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas.

¹²⁰ Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas (Žin., 2011, Nr. 52-2511).

¹²¹ Lietuvos Aukščiausiojo Teismo civilinė byla E3K-3-472-916/2017.

Su dirbtinio intelekto, konkrečiai – veido atpažinimo technologijų, naudojimu ir biometrinėmis duomenimis tvarkymu susijusi 2022 m. gegužės 13 d. Vilniaus apygardos administracinių teismo byla¹²², kurioje šis teismas nusprendė, kad Vilniaus universiteto sprendimas egzaminų metu naudotis veido atpažinimo SMOWL programine įranga pripažintinas kaip proporcingsas tuo metu visoje šalyje buvusios ekstremalios situacijos (dėl COVID-19 pandemijos) kontekste, o biometrinėmis duomenimis tvarkymas atitinko BDAR įtvirtintas išimtines duomenų tvarkymo sąlygas. SMOWL yra programinė įranga („Moodle“ įskiepis), kuris automatiškai stebi studentus egzamino (testo) metu per jų kompiuterio kameras ir mikrofonus. Likus 72 val. iki egzamino (testo), studentai turi internetu užsiregistravoti SMOWL sistemoje, jie ir jų studento pažymėjimai yra nufotografuojami per jų pačių kameras. Iš šių duomenų sistema sudaro biometrinius studentų veido modelius, pagal kuriuos atpažįsta studentus egzamino (testo) metu. Egzamino (testo) metu renkamos nuotraukos per kamerą ir, esant pašaliniam garsams, įrašomas garsas per mikrofoną. Taip pat iki egzamino (testo) studentai savo kompiuteriuose turi instaluoti specialias programas, kurios stebi, kokie langai yra atidaryti kompiuteriuose atsiskaitymo metu¹²³.

Šioje byloje teismas konstatavo, kad Vilniaus universiteto pasirinkimą atsiskaitymus organizuoti taikant veido atpažinimo funkciją lėmė ne įstaigos siekis patogumo ar ekonomiškumo, o būtinybė dėl šalyje susidariusios kritinės situacijos dėl COVID-19 pandemijos, ir tai atitinka BDAR 9 straipsnio 2 dalies a punkte įtvirtintą sąlygą – jei buvo gauti studijuojančių asmenų sutikimai ir papildomai 9 straipsnio 2 dalies g punkte nustatytą išimtinę sąlygą – dėl svarbaus viešojo intereso priežasčių. Idomu tai, kad šioje byloje teismas išsamiai apsvarstė būtinybę naudoti veido atpažinimo technologijas dėl COVID-19 pandemijos, tačiau iš esmės nebuvo svarstyta su šios priemonės proporcingu susijęs klausimas – ar iš tiesų nebuvo jokių kitų alternatyvų vykdysti nuotolinis egzaminus, išskyrus vykdymą naudojant veido atpažinimo technologijas arba nukeliant egzaminą neiškiam terminui jį laikyti kontaktiniu būdu. Suprantama, kad programas SMOWL naudojimas užtikrinant, kad nebūtų pašalinių garsų egzamino metu ar kad studentas nebūtų atsidaręs kitų kompiuterio langų, yra reikalingas siekiant užtikrinti sąžiningumą laikant egzaminą. Tačiau argumentas, kad veido atpažinimo technologijų naudojimas buvo vienintelė alternatyva atpažinti, kad būtent konkretus studentas laiko egzaminą (atsiskaitymą), o ne pašalinis asmuo, neatrodė iki galio įtikinamai, ypač atsižvelgiant į tai, kad, laikant egzaminą kontaktiniu būdu,

¹²² Vilniaus apygardos administracinių teismo 2022 m. gegužės 12 d. administracinė byla Nr. eI3-839-809/2022.

¹²³ Vilniaus universiteto Medicinos fakulteto informacija. Prieiga per internetą: https://www.mf.vu.lt-/images/Remiantis_Vilniaus_universiteto_Medicinos_fakulteto_tarybos_2021.pdf.

nėra naudojamas veido atpažinimo technologijomis, kad būtų įsitikinta studento tapatybė – dėstytojui užtenka patikrinti veido panašumą su nuotrauka asmens dokumente. Kyla klausimas, kodėl laikant egzaminą nuotoliniu būdu nepakaktų, siekiant įsitikinti, kad egzaminą laiko tas pats asmuo, jog dėstytojas pats palygintų asmenį per ekraną laikantį egzaminą, su jo nuotrauka dokumente, tačiau teismas šio aspekto nesvarstė.

Kalbant apie asmens duomenų tvarkymą Lietuvos teisėsaugos institucijoje, kur yra ar gali būti naudojamas dirbtinis intelektas, konkretius duomenų tvarkymo pagrindus nustato atskirų institucijų veiklą ar atskiras veiklos sritis reguliuojantys įstatymai.

Kai kuriuose teisės aktuose nustatyta pareiga tvarkant asmens duomenis ar naujodant pažangias technologijas duomenims tvarkyti laikytis bendruųjų teisės aktų reikalavimų. Pavyzdžiui, Lietuvos Respublikos baudžiamojo proceso kodekse nustatyta, kad techninių priemonių panaudojimo rezultatai negali būti naudojami taip, kad būtų pažeistas kitų asmenų teisės ar kiti įstatymų saugomi interesai arba būtų iškraipytas teismo sprendimo turinys ar esmė, taip pat negali būti naudojami politinės ar kitokios reklamos, satyros, pramogų ir kitais su pagarba teismui nesuderinamais tikslais. Techninių priemonių panaudojimo rezultatams ir jų naudojimui taip pat taikomi kituose įstatymuose nustatyti visuomenės informavimo, asmens duomenų apsaugos, teisės į privataus gyvenimo neliečiamumą bei asmens garbės ir orumo apsaugos reikalavimai¹²⁴. Tai reiškia, kad baudžiamajame procese naudojant dirbtiniu intelektu grindžiamas priemones turi būti atsižvelgiama į minėto Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo užjas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo reikalavimus. Greičiausiai dėl šios priežasties daugelyje¹²⁵ kitų įstatymų, kurie yra taikomi atliekant baudžiamojo proceso veiksmus, konkretiai – Lietuvos Respublikos prokuratūros įstatyme¹²⁶, Lietuvos Respublikos finansinių nusikalstamų tyrimo tarnybos įstatyme¹²⁷, reikalavimas atsižvelgti į bendruosius asmens duomenų, įskaitant biometrinį duomenų, tvarkymo reikalavimus dalyvaujant baudžiamajame procese nėra numatytas.

Nors galima daryti prielaidą, kad pakartotinai įstatymuose net ir nereikia minėti, kad duomenų apsaugos, įskaitant biometrinius duomenis, reikalavimai yra taikomi

¹²⁴ Lietuvos Respublikos baudžiamojo proceso kodekso (Žin., 2002, Nr. 37-1341) 260 straipsnio 4 dalis.

¹²⁵ Išimtis būtų Lietuvos Respublikos kriminalinės žvalgybos įstatymas, kuriame numatyta: „Kriminalinės žvalgybos metu negali būti pažeistos žmogaus teisės ir laisvės. Atskiri šių teisių ir laisvių ribojimai yra laikini ir gali būti taikomi tik įstatymų nustatyta tvarka, siekiant apginti kito asmens teises ir laisves, nuosavybę, visuomenės ir valstybės saugumą.“ Žr. Lietuvos Respublikos kriminalinės žvalgybos įstatymo (Žin., 2012-10-20, Nr. 122-6093) 5 straipsnio 1 dalį.

¹²⁶ Lietuvos Respublikos prokuratūros įstatymas (Žin., 1994, Nr. 81-1514).

¹²⁷ Lietuvos Respublikos finansinių nusikalstamų tyrimo tarnybos įstatymas (Žin., 2002, Nr. 33-1250).

visoms viešojo sektoriaus institucijoms, tačiau reguliacinį nenuoseklumą šioje srityje galima ižvelgti. Pavyzdžiu, policijos veikla yra platesnė nei tik dalyvavimas baudžiamajame procese, tačiau Lietuvos Respublikos policijos įstatyme nėra nuostatų dėl būtinumo laikytis duomenų apsaugos reikalavimų, nors yra numatyta, kad policijos pareigūnas, atlikdamas jam pavestas funkcijas, gali asmens sutikimu ir (ar) įstatymu nustatytais atvejais fotografioti, daryti garso ar vaizdo įrašus, taip pat be asmens sutikimo policijos generalinio komisaro nustatyta tvarka fotografioti asmenis, kurių tapatybę nenustatyta, bejegiškos būklės asmenis, neatpažintus lavonus, rizikos grupės asmenis, laikinai sulaikytus asmenis, juos matuoti, aprašyti jų išorės požymius, daryti garso ar vaizdo įrašus, imti pirštų atspaudus, ēminius genetiniams tipizavimui ar pavyzdžius lyginamajam tyrimui ir identifikavimui atliskti, taip pat tvarkyti šiuos duomenis¹²⁸. Įstatyme taip pat numatyta, kad policijos pareigūnai gali be duomenų subjekto sutikimo tvarkyti būtinus policijos uždaviniams įgyvendinti asmens duomenis bei kad tvarkydama duomenis policija turi teisę juos rinkti naudodama technines priemones¹²⁹.

Bausmių vykdymo kodekse numatyta, kad, vykdymada viešujų darbų bausmę, probacijos tarnyba turi teisę neatlygintinai gauti iš valstybės, savivaldybių ir kitų institucijų, įstaigų, organizacijų valstybės informacinių išteklių duomenis ir dokumentus bei kitą informaciją, reikalingus viešujų darbų bausmei įvykdysti, arba susipažinti su šia informacija bei tvarkyti nuteistujų asmens duomenis¹³⁰, tačiau reikalavimas paisyti duomenų apsaugos reikalavimo taip pat nėra numatytas. Panašus reguliavimas numatytas ir kituose įstatymuose. Pavyzdžiu, Lietuvos Respublikos žvalgybos įstatyme įtvirtinta, kad žvalgybos institucijos turi teisę tvarkyti asmens duomenis¹³¹. Taip pat kad vykdant žvalgybos veiklą galimi šie veiksmai – elektroninių ryšių tinklais perduodamos informacijos turinio, susirašinėjimo ir kitokio asmens susižinojimo stebėjimas ir fiksavimas; patekimas į asmens būstą, kitokias patalpas ar transporto priemones, jų apžiūra ir fiksavimas; dokumentų ar daiktų paémimas ar slapta jų apžiūra ir fiksavimas; informacijos apie elektroninių ryšių įvykius gavimas; pinigų, piniginių srautų, vertybinių popierių, elektroninių ir kitų atsiskaitymo būdų, taip pat bet kokių finansinių operacijų stebėjimas ir fiksavimas; informacijos apie fizinių ir (ar) juridinių asmenų iki teikimo teismui gauti tokią informaciją pateikimo atliskas ūkines, finansines operacijas, finansinių ir (ar) mokėjimo priemonių panaudojimą gavimas iš finansų įmonių ir kredito įstaigų, taip pat iš kitų juridinių asmenų. Tiesa, šie veiksmai lei-

¹²⁸ Lietuvos Respublikos policijos įstatymo (Žin., 2000, Nr. 90-2777) 22 straipsnio 1 dalis.

¹²⁹ Policijos įstatymo 9 straipsnio 1 ir 2 dalys.

¹³⁰ Lietuvos Respublikos bausmių vykdymo kodekso (Žin., 2002, Nr. 73-3084) 43 straipsnio 1 dalis.

¹³¹ Lietuvos Respublikos žvalgybos įstatymo (Žin., 2000, Nr. 64-1931) 9 straipsnio 2 dalis.

džiami tik gavus apygardos administracino teismo leidimą¹³². Daugiau jokių sąlygų dėl duomenų rinkimo ar tvarkymo įstatyme nėra nurodoma, todėl darytina išvada, kad šias sąlygas, taip pat, kur taikoma, ir biometrinių duomenų tvarkymo sąlygas turėtų įvertinti teismas išduodamas leidimą minėtiems veiksmams. Administracinių nusižengimų kodekse¹³³ numatyta, kad administracino nusižengimo tyrimo veiksmų metu gali būti fotografuojama, filmuojama, daromas garso ir vaizdo įrašas, daromi pėdsakų atspaudai ir išliejos, sudaromi planai ir schemas ir naudojami kitokie fiksavimo būdai¹³⁴. Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatyme numatyta, kad vykdant tyrimą šios tarnybos pareigūnai gali iš valstybės ir savivaldybių institucijų, įstaigų ir įmonių, valstybės ir savivaldybių valdomų įmonių, įmonių, kurių akciniukė yra valstybė ar savivaldybė, viešujų įstaigų, kurių steigėja, savininkė ar dalininukė yra valstybė ar savivaldybė, neatlygintinai gauti Specialiųjų tyrimų tarnybos funkcijoms atliliki reikalingus valstybės informacinių ištaklių duomenis ir dokumentus bei kitą informaciją. Be to, šiame įstatyme netiesiogiai paminėta ir Specialiųjų tyrimų tarnybos teisė savo analitinės antikorupcinės žvalgybos veikloje naudoti ir su kitomis institucijomis dalintis specialia technika apdorotais duomenimis – remiantis įstatymu, analitinė antikorupcinė žvalgyba – Specialiųjų tyrimų tarnybos vykdoma analitinė veikla, apimanti informacijos apie korupciją ir su ja susijusius reiškinius rinkimą, apdorojimą, gretinimą su kita Specialiųjų tyrimų tarnybos turima vieša ar įslaptinta informacija, kokybiškai naujų duomenų, kurie yra šių informacijos apdorojimo procesų rezultatas, gavimą, naudojimą ir teikimą valstybės ar savivaldybės institucijoms ir pareigūnams, įgaliojimams priimti korupcijos paplitimo mažinimo požiūriu reikšmingus sprendimus¹³⁵. Taigi, įstatymas nenumato konkrečių taisyklių, tik užsimena, kad Specialiųjų tyrimų tarnyboje gali būti naudojamos dirbtinio intelekto sistemos, tačiau jokie konkretūs kriterijai, kada ir kokiomis sąlygomis tas galėtų būti daroma, bei biometrinių duomenų tvarkymo pagrindai nėra aprašyti. Taip pat tam tikros tai-sykles dėl biometrinių duomenų tvarkymo nustatytos asmens dokumentų išdavimą ir migraciją reguliuojančiuose teisės aktuose¹³⁶. Tačiau atsižvelgiant į tai, kad šioje

¹³² Žvalgybos įstatymo 13 str. 1 d.

¹³³ Lietuvos Respublikos administracinių nusižengimų kodeksas (TAR, 2015, Nr. 11216).

¹³⁴ Administracinių nusižengimų kodekso 594 str. 1 d.

¹³⁵ Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatymo (Žin., 2000, Nr. 41-1162) 8 straipsnio 1 dalis ir 9 straipsnis.

¹³⁶ Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas (TAR, 2014, Nr. 21281); Lietuvos Respublikos įstatymas dėl užsieniečių teisinės padėties (Žin., 2004-04-30, Nr. 73-2539); Lietuvos Respublikos tarnybinio paso įstatymas (Žin., 2000, Nr. 7-178); Lietuvos Respublikos vidaus reikalų ministro įsakymas dėl motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo (Žin., 2008, Nr. 106-4060) ir t. t.

srityje klausimų dėl asmens privatumo iš esmės (išskyrus pavienius atvejus) nekyla, šioje studijoje šie klausimai nebus išsamiau analizuojami.

Apibendrinant galima pastebėti, kad teisės aktuose įtvirtintos nuostatos, reguliuojančios galimybę rinkti ir tvarkyti asmens duomenis, įskaitant biometrinius duomenis, bei kitaip kištis į asmenų privatų gyvenimą, yra gana fragmentuotos ir nenuoseklios. Daugeliu atvejų tik nurodoma, kad teisėsaugos institucijos turi teisę rinkti ir tvarkyti asmens duomenis, tačiau nėra pateikiami kriterijai, kada ir kaip tai gali būti atliekama. Kalbant apie šių nuostatų taikymą asmenų atžvilgiu, konstatuotina, kad minėtų įstatymų nuostatos gali būti taikomos ne tik asmenims, padariusiems nusikalstamas veikas ar administracinius nusižengimus, dalyvaujantiems migracijos procesuose, asmenims, susijusiems su kriminaline žvalgyba ar nacionaliniu saugumu, bet ir bet kuriems kitiems asmenims, kurie pasirodo viešose vietose.

Asmens duomenų rinkimą taip pat reguliuoja ir savivaldybių patvirtintos taisyklės dėl vaizdo stebėjimo viešose vietose¹³⁷. Tokios vaizdo stebėjimo kameros įrengiamos turint tikslą „užtikrinti asmens, visuomenės saugumą ir viešąjį tvarką savivaldybės teritorijoje, pagal kompetenciją fiksuoći teisės pažeidimus, naudoti vaizdo stebėjimo metu gautus duomenis atskleidžiant ir tiriant administracinius nusižengimus, vadovaujantis Lietuvos Respublikos administracinių nusižengimų kodeksu, naudoti vaizdo stebėjimo metu gautus duomenis atskleidžiant ir tiriant nusikalstamas veikas, vadovaujantis Lietuvos Respublikos baudžiamojo proceso kodeksu ir vykdyti nusikalstamą veiką ir administracinių nusižengimų prevenciją“. Šios taisyklės grindžiamos Lietuvos Respublikos vienos savivaldos įstatymo nuostatomis, suteikiančiomis vienos savivaldos institucijoms pagal savo kompetenciją priimti privalomus sprendimus¹³⁸. Šios taisyklės nekalba apie tai, kad duomenys gali būti apdorojami specialiu būdu ir gaunami asmenų biometriniai duomenys, tačiau tai įmanoma padaryti, jei šie duomenys bus perduoti kitoms institucijoms, kurios turi techninių galimybių tai atliliki.

Atsižvelgiant į tai, kad galima atskirai fiksuoći veido atvaizdą ir tokią asmens duomenų tvarkymui taikomos įprastinės duomenų tvarkymo taisyklės, tačiau jei šis atvaizdas bus apdorotas veido atpažinimo technologijų programa, yra svarbu, kam ir

¹³⁷ Pvz., žr. Šiaulių miesto savivaldybės tarybos įsakymą „Dėl Šiaulių miesto savivaldybės teritorijoje įrengtų vaizdo stebėjimo kamerų ir jų fiksuočių duomenų rinkimo ir naudojimo taisyklės patvirtinimo“ (TAR, 2020, Nr. 10216); Kaišiadorių rajono savivaldybės tarybos įsakymą „Dėl Kaišiadorių rajono savivaldybės teritorijoje įrengtų vaizdo stebėjimo kamerų ir jų fiksuočių duomenų naudojimo tvarkos aprašo patvirtinimo“ (TAR, 2022, Nr. 13200); Tauragės rajono savivaldybės tarybos įsakymą „Dėl Tauragės rajono savivaldybės viešosių įrengtų vaizdo stebėjimo kamerų ir jų fiksuočių duomenų naudojimo tvarkos aprašo patvirtinimo“ (TAR, 2022, Nr. 7557) ir kt.

¹³⁸ Lietuvos Respublikos vienos savivaldos įstatymo (Žin., 1994, Nr. 55-1049) 29 straipsnio 8 dalies 2 ir 3 punktai.

3. PRIVATUMO IR ASMENS DUOMENŲ SAMPRATA DIRBTINIO INTELEKTO KONTEKSTE

kokiais atvejais veido atvaizdas bus perduotas. Kitaip tariant, jei asmens veido atvaizdas patenka į tam tikrą duomenų bazę, yra rizika, kad, esant duomenų susiejimui tarp duomenų bazių, veido atvaizdas bus apdorotas specialia įranga ir taps biometriniais duomenimis.

Remiantis Lietuvos Respublikos teisės aktais, teisėsaugos veikloje tvarkomi asmenų veido atvaizdai laikomi įvairiose institucijų duomenų bazėse, kurios yra susietos tarpusavyje – Policijos informacijos sistemoje (POLIS) ir kituose žinybiniuose policijos padalinių registruose, Kriminalinės žvalgybos informacinėje sistemoje, sulaikymo ir laisvės atėmimo įstaigų duomenų bazėse, teismų ir kitų institucijų duomenų bazėse, taip pat valstybės įmonės „Regitra“ duomenų bazėse, įvairiuose savivaldybių registruose ir t. t.¹³⁹.

¹³⁹ Žr. Legal Analysis for TELEFI project Towards the European Level Exchange of Facial Images. Prieiga per internetą: https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf.

4. DIRBTINIO INTELEKTO NAUDOJIMO KELIAMOS GRĘSMĖS PRIVATUMUI

Kaip buvo aptarta šios studijos 2 skyriuje, vis didesnis dirbtinio intelekto technologijų naudojimas kelia įvairių grėsmių individams ir visuomenei. Šioje studijos dalyje, atsižvelgiant į Europoje ir Lietuvoje teisės aktuose ir teismų praktikoje nurodytas teisės į privatumo ir teisės į duomenų apsaugą ribas, bus siekiama sugrupuoti dirbtinio intelekto technologijų keliamus pavojujus šioms žmogaus teisėms.

4.1. Dirbtinio intelekto pagalba renkant asmens duomenis

Viena iš sričių, kur pasitelkiamos dirbtinio intelekto technologijos, yra įvairių duomenų rinkimas. Duomenys renkami labai įvairiai tikslais – tiek siekiant gauti pakan-kamai informacijos, reikalingos tam tikriems sprendimams priimti, tiek siekiant nustatyti tam tikras tendencijas, atliki profiliavimą ir t. t. Duomenys renkami tiek turint tikslą juos panaudoti užprogramuojant užduotis dirbtiniams intelektui (t. y. nustatyti sąlygas, pagal kurias dirbtinis intelektas turės priimti sprendimą, pavyzdžiu, naudojant „ekspertines sistemas“, kaip apibūdinta šios studijos 1 skyriuje), tiek suteikiant duomenis, kad dirbtinis intelektas pats galėtų identifikuoti tam tikras tendencijas iš turimų duomenų srauto (mašininio mokymosi, išskaitant giluminį mokymąsi ir neuroninius tinklus, atvejaus). Natūralu, kad kuo toliau, tuo daugiau dirbtinis intelektas naudojamas kaip savarankiškai priimantis sprendimus ar net nusistatantis sau tikslus, remdamasis turimais duomenimis. Vadinas, kuo daugiau bus plėtojamos dirbtinio intelekto sistemos, tuo daugiau duomenų tam reikės.

Duomenų rinkimas, ypač neribojamo masto duomenų rinkimas, kelia keleriopų grėsmių asmens privatumui.

Kalbant apie privataus pobūdžio duomenų rinkimą, galima išskirti kokybinius ir kiekybinius pokyčius, atsirandančius ir toliau tobulinamus kartu su dirbtinio intelekto kūrimo ir naudojimo plėtra. Pirma, tobulėja pačios technologijos. Pavyzdžiu, vis labiau tobulinama vaizdo kamerų filmuojamos medžiagos kokybė – vaizdo duomenų

rezoliucija, rezultatai filmuojant tamsoje ar esant blogoms oro sąlygoms, dėl to, pa-vyzdžiui, iš toli galima identifikuoti ne tik ką asmuo apsirengęs, bet ir kokio prekinio ženklo ir kokio susidėvėjimo yra jo drabužiai, batai, turimi daiktai, jei kažkas kyšo iš kišenės, tinkamai pritraukus vaizdą taip pat galima bent jau kelti hipotezes, kas ten yra. Tas pats pasakytina ir apie garso įrašų kokybės tobulėjimą, asmens buvimo vietas nustatymo tikslumą ir pan. Antra, plėtojant technologijų ir dirbtinio intelekto gali-mybes, galima rinkti vis įvairesnius duomenis apie asmenis. Pavyzdžiui, prieš porą dešimtmečių duomenų apie asmenį rinkimas buvo labai ribotas – iš esmės buvo galima tik filmuoti, fotograuoti ar daryti garso įrašus – visas kitas duomenų rinkimas buvo tik su asmens ar kitų asmenų tiesioginiu dalyvavimu (pvz., kai jis pats pasirašo, pateikia ar registruoja dokumentus, yra „susiskaičiuojamas“, rankiniu būdu fiksuoja-ma jo sveikatos ir kt. istorija, ir pan.). Dabar egzistuoja įvairiausią būdų rinkti duo-menis apie asmenis – pradedant vaizdo stebėjimo kameromis ir fotografijomis, garso įrašymu, banko ar mokėjimo sąskaitos, mokėjimo kortelės duomenų fiksavimas, taip pat fiksavimas, kam ir iš kur jis gauna lėšas, medicininių duomenų automatizuotas fiksavimas, kūno būklės, fizinio pajėgumo, nuotaikų, elgesio, nuolatinio širdies ritmo, deguonies kiekio, miego trukmės ir kokybės, automatizuotas žingsnių stebėjimas ir fiksavimas, mobiliojo ryšio duomenų srautas, kuris nusako, kur, su kuo ir kada buvo kalbėta telefonu, kokios žinutės buvo rašytos, taip pat asmens buvimo vietas, įprasti-nių ir neįprastų maršrutų, judėjimo greičio nustatymas remiantis GPS duomenimis, slapukų naudojimas fiksujant naršymo internete, televizijos žiūréjimo, muzikos klau-symo duomenis ir t. t.¹⁴⁰ Galiausiai yra svarbu, kaip ir kokiu būdu šie duomenys yra renkami – kada jie fiksujami, kiek laiko saugomi, kas prie jų turi prieigą ir t. t. Dirbtinis intelektas įgalina svarbiais laikyti ne visus, bet tam tikrus asmens duomenis. Pavyzdžiui, fiksuoти jo pokalbius telefonu tik tada, kai skamba tam tikri raktiniai žo-džiai; įrašyti vaizdo priemonėmis fiksujamus tik tų asmenų, kurie atitinka tam tikrus kriterijus, duomenis ir t. t.

Šiame kontekste paminėtina, kad renkant asmens duomenis turėtų būti laikomasi tiek Europos Sajungoje aiškiai nustatyto būtinumo ir proporcingumo reikalavimo, tiek ir Bendrojo duomenų apsaugos reglamento principų – teisėtumo, sąžiningumo ir skaidrumo; tiksloto apribojimo; duomenų kiekio mažinimo ir t. t. Tačiau šioje vietoje šių principų taikymas yra siek tiek keblus – iš esmės būtinumo ir proporcingumo rei-kalavimas taikomas tik kai yra kišamasi į asmens privatų gyvenimą, tačiau duomenų rinkimo kontekste tai yra aktualu tik kalbant apie kokybinį duomenų rinkimą – kai

¹⁴⁰ Council of Europe. Algorithms and Human Rights. DGI, 2018, p. 12. Prieiga per internetą: <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

renkant duomenis jų tikslumas yra tokis, kad jau yra įsibraunama į privatų asmens gyvenimą (pvz., galima ižvelgti, ką asmuo nešasi kišenėje arba kas matyti jo balkone ar kambaryje per užuolaidas). Duomenų rinkimas remiantis Bendruoju duomenų apsaugos reglamento irgi gali būti pateisinamas, kadangi reikalavimai yra taikomi kiekvienu konkrečiu atveju, ir gali būti, kad visais atvejais asmuo arba pats duoda sutikimą jo duomenų naudojimui (pvz., pats naudoja išmanujį laikrodį, sekantį jo miego ir aktyvumo duomenis ir iopročius; neišvengiamai priverstas duoti sutikimą tam, kad būtų atliktas jo medicininis tyrimas ir t. t.), arba to reikia viešojo intereso tikslais (pvz., vaizdo kamera stebi viešąsias vietas, kur vyksta daug nusikalstamų veikų), arba tai yra būtina dėl kitų priežasčių. Tol, kol gausybė asmens duomenų nėra sujungiama tarpusavyje, teisės į privatumą bei duomenų apsaugos teisiniai saugikliai neįsijungia, nes masinis duomenų rinkimas iš esmės yra tik prielaidos galimam žmogaus ar žmonių grupės teisių pažeidimui. Taigi, iš esmės grėsmė privatumui šiuo atveju kyla tik dėl to, jog kuo daugiau duomenų apie asmenį yra fiksuojama ir tvarkoma, tuo didesnė egzistuoja techninės klaidos tvarkant asmens duomenis tikimybė, arba tie duomenys gali būti tikslingai nutekinami, arba sujungti tarpusavyje, o tai savaime yra kitas dirbtinio intelekto naudojimo tvarkant asmens duomenis pavojuς, aptariamas tolesniame šios studijos poskyryje. Šiame kontekste paminėtinas jau cituotas Konstitucinio Teismo išaiškinimas, jog asmens teisė į jo privataus gyvenimo gerbimą ir šios teisės apsauga aiškintina plečiamai, atsižvelgiant *inter alia* į mokslo ir technologijų pažangą, su teikiančią vis daugiau galimybių kištis į asmens privatų gyvenimą, kaip antai nusikalstamų veikų prevencijos ar kitais viešosios tvarkos apsaugos tikslais renkant, kaupiant, naudojant ir saugant ne tik asmens pirštų atspaudų, jo balso, bet ir asmens ląstelių ar DNR mėginių pavyzdžius, technikos priemonėmis masiškai stebint ir sekant asmenų naudojamas elektronines erdves, *inter alia* pasitelkus globalinės padėties nustatymo sistemą (GPS) nustatant asmenų buvimo vietą¹⁴¹. Taigi labai svarbu, kad, didėjant galimybėms ir būdams fiksuoti ir tvarkyti asmens duomenis, didėja būtinybė vis daugiau dėmesio skirti užtikrinimui, kad duomenys bus tvarkomi tik izoliuotai vieni nuo kitų ir tikslingai, remiantis Bendrojo duomenų apsaugos reglamento reikalavimais.

Šiame kontekste paminėtinas ir „didžiųjų duomenų“ (angl. *big data*) atvėrimo skatinimas demokratinėse valstybėse. Viena vertus, reikia sutikti, kad duomenų atvėrimas didina skaidrumą, ypač kai atveriami duomenys susiję su viešaisiais asmenimis, tačiau kai šių duomenų atveriamas vis daugiau, asmenys gali nukentėti nuo nusikaltėlių, kurie galės teisėtai agreguoti viešai skelbiamus duomenis ir tai jiems padės planuoti nusikalstamas veikas, antra vertus, tai sudaro galimybę ne tik nacionalinės val-

¹⁴¹ Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas.

džios institucijoms, bet ir priešiškų valstybių žvalgybos institucijoms teisėtai gauti ir agreguoti informaciją apie asmenis, kuria remdamies jie galės juos greičiau užverbuoti neteisėtoms veikoms prieš savo valstybę vykdyti.

4.2. Veido atpažinimo sistemų naudojimas

Kaip jau buvo minėta, veido atpažinimo sistemos leidžia aptikti veidus (tokia technologija visiškai nesusijusi su privatumo pažeidimu), apibūdinti veidus (nustatyti rasę, etninę kilmę, asmens emocijas ir t. t. – tokia technologija sudaro prielaidas asmenis profiliuoti), patvirtinti asmenis (atliki 1:1 tapatybės patvirtinimą, t. y. patvirtinti asmens tapatybę pagal jau užfiksotą biometrinių duomenų kodą) ir identifikuoti asmenis (atliki 1:n identifikavimą, t. y. palyginti asmens biometrinius duomenis su didele biometrinių duomenų baze, siekiant nustatyti, kuris asmuo iš daugelio galimų tai yra).

Veido atpažinimo technologijų yra įvairių – jos grindžiamos ir skirtingomis turimomis asmenų biometrinių duomenų bazėmis (pvz., duomenys apie asmenis surinkti iš viešai prieinamų šaltinių, įskaitant socialinius tinklus, pvz., „Clearview“¹⁴², duomenys iš valstybės registru, t. t.), skirtingais tikslumo nustatymo procentiniais punktais (pvz., skirtingu gebėjimu pateikti tikslų rezultatą priklausomai nuo to, kokios etinės kilmės ar lyties yra asmuo), skirtinga skiriamaja raiška ir t. t. Tačiau žvelgiant iš asmens teisės į privatumą perspektyvos ir suderinamumo su dabartine teisine sistema yra svarbi skirtis tarp vaizdo stebėjimo įrangos, gebančios identifikuoti asmenis realiu laiku (angl. *real-time*), ir vaizdo stebėjimo įrangos, gebančios identifikuoti asmenį iš filmuotos ar fotografuotos medžiagos. Kaip jau buvo minėta, biometriniams asmens duomenims taikomas specialus ir griežtesnis apsaugos režimas nei įprastiems asmens duomenims. Pagal teisės aktuose įtvirtintus apibrėžimus, biometriniai duomenys – tai po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys¹⁴³. Pagal Bendrajį duomenų apsaugos reglamentą (kartu ir Duomenų apsaugos teisėsaugos srityje direktyvą), biometriniai duomenys yra tik tie duomenys, kurie specialiai techniškai apdoroti. Taigi, tokie asmens duomenys, kaip veido atvaizdas, balsas, eisena bei kiti bruožai, kol nėra apdoroti specialiomis priemonėmis, yra laikomi „paprastais asmens duomenimis“ ir jiems netai komas biometrinių duomenų apsaugos režimas.

¹⁴² Clearview AI principles. Prieiga per internetą: <https://www.clearview.ai/principles>.

¹⁴³ BDAR 4 straipsnio 14 punktas, Teisėsaugos direktyvos 3 straipsnio 13 dalis.

Tai yra svarbu atsižvelgiant į tai, kad galima atskirai fiksuoti veido atvaizdą, ir tokių asmens duomenų tvarkymui taikomos įprastinės duomenų tvarkymo taisyklės. Dar daugiau – kaip jau minėta, viešoje vietoje fotografuoti asmenis galima ir be jų sutikimo¹⁴⁴. Tačiau jei šis atvaizdas bus apdorotas veido atpažinimo technologijų programa, jam turės būti taikomos biometrinių duomenų tvarkymo taisyklės.

Taigi, problema kyla dėl to, kad veidų fiksavimas viešoje vietoje naudojant įprastines vaizdo fiksavimo priemones nėra draudžiamas ar griežtai ribojamas. Didžiausias dėmesys siekiant užtikrinti asmenų teisę į privatumą (t. y. teisę būti neatpažintiems) ir biometrinių duomenų apsaugą turėtų būti skiriamas atsižvelgiant į tai, kokia technologija yra naudojama duomenų apdorojimui.

Tiek Europos Žmogaus Teisių Teismas (pvz., jau aptartoje *Liberty* byloje), tiek Konstitucinis Teismas (pvz., Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas) yra pabrėžę, kad svarbu yra asmenį informuoti apie duomenų apie jo privatų gyvenimą rinkimą. Šią reikalavimą yra ypač sunku įgyvendinti tais atvejais, kai asmens vaizdo duomenų fiksavimas ir jų apdorojimas vyksta skirtingu metu ir gali priklausyti nuo skirtinės aplinkybių. Pavyzdžiui, kai asmuo yra nufilmuotas viešoje vietoje „paprasta“ vaizdo fiksavimo kamera, tačiau dėl tam tikrų priežasčių prireikus jo veidas yra apdorojamas naudojantis veido atpažinimo technologijomis. Vadinas, siekiant tinkamai užtikrinti asmenų teisę į privatumą, asmuo turėtų būti arba iš anksto informuojamas apie tai, jog galimai jo biometriniai duomenys bus tvarkomi vėliau, arba ši informacija asmeniui turėtų būti pateikiama prieš ar iškart po jo atvaizdo apdorojimo veido atpažinimo technologijomis.

4.3. Asmens duomenų sujungimas ir agregavimas

Kaip buvo minėta anksčiau šiame studijos skyriuje, duomenų apie asmenis, jų įpročius, fizinius ir emocinius bruožus ir savybes rinkimas vis labiau intensyvėja, be to, tobulėjant technologijoms, renkami vis įvairesni asmens duomenys. Tai kelia didelę grėsmę, kad, sujungus daug įvairių duomenų apie tą patį asmenį, nukentės jo privatumas. Kaip nurodė Europos Žmogaus Teisių Teismas, pasiskydamas apie valdžios institucijų veiklą, tai, jog valdžios institucijos turi galimybę gauti išsamią asmeninio pobūdžio informaciją apie asmenį sujungdamos duomenis iš įvairių šaltinių, laikytina ypač dideliu kišimusi į asmeninį gyvenimą¹⁴⁵.

¹⁴⁴ Civilinio kodekso 2.22 straipsnis.

¹⁴⁵ Szabó ir Vissy prieš Vengriją, 70 punktas.

Įvairių asmens duomenų sujungimas sudaro prielaidas įvairiais būdais pažeisti asmens teisę į privatumą. Pavyzdžiui, kaip jau minėta, jei tokiai duomenimis disponuoja nusikalsteliai, jie gali nedelsdami suplanuoti asmens apiplėšimą, vagystę, pinigų pasisavinimą elektroniniu būdu ar kitą nusikalstamą veiką. Valstybės institucijos, turėdamos neribotą kiekį duomenų apie tą patį asmenį, gali ji sekti ir riboti jo politinę ir saviraiškos laisvę. Būtent dėl šio aspekto demokratinės visuomenės priešinasi viešosios valdžios iniciatyvoms rinkti asmens duomenis, ypač trūkstant skaidrumo, kaip šie duomenys yra agreguojami tarpusavyje.

Be to, remiantis duomenų aggregavimu vykdomas asmenų profiliavimas. Pavyzdžiui, dirbtinis intelektas nemažai naudojamas siekiant užkirsti kelią nusikalstamui – policijos veikloje vis dažniau vartojamas terminas „nuspėjamoji policijos veikla“ (angl. *predictive policing*) – t. y. policijos veiksmai grindžiami prielaida, kad, pasitelkus dirbtinį intelektą, tinkamai naudojant tiksliai parinktus algoritmus, galima nuspėti, kuriose vietovėse ir kokie asmenys gali daryti nusikalstamas veikas, ir užkirsti tam kelią¹⁴⁶. Nuspėjamosios policijos veiklos ištakos gali būti siejamos su kompiuterinės nusikalstamumo kontrolės eksperimentais aštuntajame dešimtmetyje, ir nors nusikaltimų ir bausmių srityje buvo kuriamos ir tobulinamos nusikalstamumo prognozės jau keletą dešimtmecčių, terminas „nuspėjamoji policijos veikla“ ilgainiui buvo susietas su didelių duomenų rinkinių (angl. *big data*) augimu. Nuspėjamoji policijos veikla gali būti labai įvairi, todėl yra išskiriamais įvairios jos rūšys. Pavyzdžiui, nuspėjamosios policijos veiklos metodus galima suskirstyti į keturias dideles kategorijas: metodai, kuriais siekiama nuspėti nusikaltimus arba numatyti vietas ir laikus su padidinta nusikalstamumo rizika; metodai, kuriais siekiama numatyti pažeidėjus arba nustatyti asmenis, kurie gali ateityje atliliki nusikalstamas veikas (arba pakartotines nusikalstamas veikas); metodai, kuriais siekiama nuspėti nusikaltelių tapatybę arba sukurti profilius, panašius į anksčiau nusikalstamas veikas padariusių asmenų profilius, ir metodai, kuriais siekiama numatyti nusikaltimų aukas. Taikant nuspėjamosios policijos veiklos metodus teisėsaugos institucijos dažnai remiasi ne tik oficialiais asmens duomenimis, kuriuos tvarko valdžios institucijos teisėsaugos srityje, bet ir privačių bendrovių įprastinėje jų veikloje renkamais duomenimis (pvz., bankininkystė, telekomunikacijos, kelionės). Be to, nuspėjamoji policijos veikla taip pat paprastai vykdoma naudojant privačių bendrovių sukurtą programinę įrangą¹⁴⁷. Kaip praneša nevyriausybinė organizacija „Amnesty International“, Jungtinės Karalystės metropoliteno policija atsisakė atskleisti informaciją, kokias kriterijais ji sudaro „žalos reitin-

¹⁴⁶ Wilson, D. Algorithmic patrol: the futures of predictive policing. In: A. Završnik (ed.). *Big Data, Crime and Social Control*. Routledge, London and New York, 2017, p. 108–127.

¹⁴⁷ Wilson, p. 114.

gus“ individualiems asmenims, ir taip pat neatskleidē, kokių konkrečiai priemonių imamas ar ketinama imtis esant vienam ar kitam „žalos reitingui“. Metropoliteno policija taip pat neatsakė paviešintus spējimus, kad ši reitingavimo sistema diskriminuoja jaunus ir juodaodžius vyrus (t. y. jų „žalos reitingas“ yra didesnis nei kitų asmenų)¹⁴⁸.

Be to, kaip pažymėjo Konstitucinis Teismas, teisė į privatumą apima ir asmens psichinį neliečiamumą¹⁴⁹. Todėl teisės į privatumą pažeidimu laikytini ir atvejai, kai pasitelkus dirbtinį intelektą taikomas individualizavimas, asmenys yra raginami ir skatinami pirkti tam tikras prekes ar paslaugas ar keisti arba stiprinti savo politines pažiūras. Dirbtinio intelekto teikiamas prekių ir paslaugų individualizavimas, kaip buvo aptarta, taikomas vienu iš dirbtinio intelekto pasiekimų – tai leidžia siūlyti asmeniui būtent tai, ko jam reikia, atsižvelgiant į jo pomėgius, apie kuriuos sužinoma iš jo interneto naršyklos istorijos, jo dažniausiai vartojamus žodžius ir posakius, jo nueitus ar nuvažiuotus maršrutus, jo išlaidas tam tikroms prekėms ar paslaugoms, taip pat į jo nuotaikas, kurios nustatomos įėjus į fizinę parduotuvę, kur yra įdiegtos veido atpažinimo technologijos su funkcija atpažinti asmens nuotaikas. Tačiau tokios informacijos rinkimas ir sugretinimas sudaro galimybes manipuliuoti asmeniu, kai jam prekės, paslaugos ar tam tikros pažiūros siūlomos būtent tada, kai jis yra pažeidžiamiausias ir jam yra sudėtingiausia atispirti nepirkus tam tikrų prekių ar paslaugų ar neatlikus kitų veiksmų (pavyzdžiui, kai asmeniui siūlomas draudimas ar teikiamas darbo pasiūlymas), kuriuos jis yra skatinamas atliglioti konkretiu metu atsižvelgiant į jo psichologinę būseną¹⁵⁰. Su manipuliavimu asmeniu, kaip jau buvo minėta, susiję ir tie atvejai, kada asmuo įtraukiamas į vaizdo žaidimus ir skatinamas perimti tų žaidimų skatinamą elgesio modelį, kai asmuo yra skatinamas klausyti konkretios muzikos, žiūrėti konkretius filmus ar serialus, rinktis konkretius naujienu kanalus. Ir nors tai nėra leidžiama remiantis teisiniais reikalavimais, kol kas nėra tiksliai apibrėžta, kur naudojant dirbtinį intelektą yra daromas psichinis poveikis ir taikomas manipuliacijos.

Galiausiai, pasitelkus dirbtinį intelektą agreguoti duomenys ne tik kad gali pažeisti asmens teisę į privatumą, bet ir pasakyti apie asmenį daugiau, nei žino jis pats ar kiti asmenys. Tikėtina, jog šio reiškinio keliamos problemos bus dar aktualesnės vis daugiau taikant „mašininį mokymąsi“. Kaip anksčiau pateiktame pavyzdyme, kai dirbtinis intelektas geriau už gydytojus gebėjo diagnozuoti pirmąsias plaučių vėžio apraiškas, visai įmanoma, kad dirbtinis intelektas, turėdamas gausybę duomenų apie konkretų asmenį, galės prognozuoti įvairias jo ligas, sutrikimus, atskleisti jo pomėgius, kuriuos galbūt jis ir pats nuo savęs slepia, ir t. t. Taigi, vienas iš netikėtų atradimų, su kuriuo

¹⁴⁸ Amnesty International, Trapped in the Matrix: Secrecy, Stigma and Bias in the Met’s Gang Database. May 2018, p. 13–14.

¹⁴⁹ Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 19 d. išvada.

¹⁵⁰ Council of Europe, p. 13.

buvo susidurta, kai dirbtinis intelektas apdoroja didelius kiekius duomenų – jis sukuria naujus duomenis apie konkretų asmenį. Tai kelia naujų iššūkių, susijusių su asmens sutikimu dėl jo duomenų tvarkymo ar kito duomenų tvarkymo pagrindo, skaidrumo ir asmens autonomijos klausimais¹⁵¹.

Net ir tuo atveju, jei asmens duomenys bus fiksuojami ir tvarkomi teisėtai, jų agregavimas ir dirbtinio intelekto gebėjimas atskleisti daug asmens savybių turint tikslą šią informaciją panaudoti įvairiais tikslais, neabejotinai yra susijęs su kišimusi į asmens privatų gyvenimą.

4.4. Sprendimų priėmimo pagrįstumas

Kaip jau buvo minėta, mašininis mokymasis pasižymi tuo, kad dirbtinis intelektas priima sprendimus ir daro prognozes naujoms situacijoms, remdamasis istoriniais duomenimis. Mašininis mokymasis grindžiamas technologija, pagal kurią mašina pati mokosi remdamasi patirtimi, negaudama jokių taisyklių ar instrukcijų iš žmonių, remdamasi tik didelio duomenų kieko tendencijomis, panašumais ir skirtumais. Naudojant tokias dirbtinio intelekto formas, kaip neprižiūrimas, sustiprintas ir gilusis mokymasis, žmogus visiškai nesikiša į dirbtinio intelekto sistemos atliekamo sprendimo priėmimo procesą.

Kai kuriais atvejais sprendimų paaiškinamumas nėra svarbus, svarbiausia – teisinės dirbtinio intelekto keliamos versijos, prognozės ar siūlomi sprendimai. Pavyzdžiui, grįžtant prie ne kartą minėto pavyzdžio apie dirbtinio intelekto pagalbą iš pirmųjų požymių diagnozuojant plaučių vėžio simptomus. Taigi, šiuo atveju svarbiausia yra rezultatas, o ne sprendimo priėmimo procesas. Tačiau kituose kontekstuose, ir ypač tai pabrėžia nevyriausybinės organizacijos, yra labai svarbu žinoti ir gebeti paaiškinti sprendimų priėmimo motyvus, tuo užtikrinant nešališkumą, atskaitingumą ir skaidrumą. Šie principai taip pat besalygiškai taikomi teisiniuose ir viešojo administruavimo santykuose – sprendimas negali būti priimtas neturint galimybės jį paaiškinti. Be to, tai ypač svarbu, kai dirbtinio intelekto sugeneruotas rezultatas turi poveikį konkretaus asmens ar asmenų grupės gerovei¹⁵². Vienas iš viešai plačiai aptarinėjamų tokų sprendimų pavyzdžių – dokumentiniame filme „Coded Bias“ pasakojama istorija apie tai, kaip 2017 metais Teksaso valstijos Hjustono mokykloje mokytojas Daniel’is Santos’as, kuris buvo gavęs nemažai apdovanojimų ir paskatinimų už gerą dar-

¹⁵¹ Council of Europe, p. 13; Stanford news. New Stanford research finds computers are better judges of personality than friends and family. Prieiga per internetą: <http://news.stanford.edu/2015/01/12/personality-computer-knows-011215/>.

¹⁵² OECD, p. 70.

bą, buvo atleistas iš mokytojo pareigų remiantis prastu jo įvertinimu, kurį atliko dirbtinis intelektas. Daniel’is Santos’as apskundė šį sprendimą, tačiau taip ir negavo atsakymo, kokiais kriterijais remiantis jo įvertinimas buvo būtent toks¹⁵³.

Taigi, su grēsmēmis asmens privatumui yra susijęs faktas, kad dirbtiniams intelektams priimant sprendimus, kai tai atliekama be žmogaus įsikišimo, nėra žinoma ir atsekmama informacija, kokiais argumentais jis remiasi ir kokius kriterijus taiko.

Kaip jau buvo minėta anksčiau, egzistuoja nuomonė, jog dirbtinio intelekto priimamieems sprendimams turėtų būti taikomas Bendrojo duomenų apsaugos reglamento 15 straipsnio 1 dalies h punktas, pagal kurį tais atvejais, kai yra priimami automatizuoti sprendimai, išskaitant profiliavimą, reikia pateikti prasmingą informaciją apie loginį sprendimo pagrindimą duomenų subjektui. Taigi, viena iš mokslininkų nuomonų yra tai, kad kai dirbtinis intelektas priima sprendimą, reikia pateikti loginį sprendimo pagrindimą, t. y. paaiškinti arba sprendimo priėmimui taikytas logikos taisykles, kitų mokslininkų teigimu, remiantis šia Bendrojo duomenų apsaugos reglamento nuostata, reikėtų paaiškinti konkretaus sprendimo priėmimo argumentaciją¹⁵⁴. Bet kuriuo atveju ir viena, ir kita atrodo sudėtinga, atsižvelgiant į tai, kad bent jau šiuo metu nėra techninių galimybių gauti paaiškinimą, kokiais principais ir argumentais remdamasis dirbtinis intelektas priėmė vieną ar kitą sprendimą.

4.5. Dirbtinio intelekto keliamos grēsmės privatumui praktikoje: Habitoskopinių duomenų registro Lietuvoje atvejis

Vienas iš pavyzdžių, kokių grēsmių asmens privatumui gali kilti nesant pakankamų saugiklių (arba kai šie saugikliai nėra viešai skelbiami) dėl aukščiau minėtų su dirbtinio intelekto naudojimu susijusių aspektų – placių galimybių rinkti asmens duomenis, veido atpažinimo technologijų įvairovės ir skirtinės funkcijų, galimybių agreguoti surinktus duomenis, yra Lietuvos habitoskopinių duomenų registro naudojimas.

Lietuvoje yra įsteigtas Habitoscopinių duomenų registras¹⁵⁵ (toliau – HDR), kurio paskirtis – kaupti duomenis, reikalingus tiriant nusikalstamas veikas ir užtikrinant jų

¹⁵³ Hay, C. Review: ‘Coded Bias,’ starring Joy Buolamwini, Cathy O’Neil, Meredith Broussard, Silkie Carlo, Ravi Naik, Zeynep Tufekci and Amy Webb. Prieiga per internetą: <https://culturemixonline.com/tag/daniel-santos/#:~:text=%E2%80%9CCoded%20Bias%E2%80%9D%20includes%20an%20inter-view%20with%20Daniel%20Santos%C,that%20was%20settled%20out%20of%20court%20in%202017>.

¹⁵⁴ Wachter et al., p. 76.

¹⁵⁵ Lietuvos Respublikos vidaus reikalų ministro 2013 m. gegužės 21 d. įsakymas Nr. 1V-440 dėl Arešto ar terminuoto laisvės atėmimo bausmė atlikusių asmenų atpažinimo žymių žinybinio registro reorganizavimo į Habitoscopinių duomenų registrą.

prevenciją, organizuojant ir vykdant asmenų paiešką, neatpažintų lavonų, nežinomų bei jėgių asmenų tapatybės nustatymą pagal asmens atpažinimo žymes bei nustatyti asmens tapatybę siekiant užtikrinti užsieniečių, kurie kompetentingų kontrolės institucijų buvo sulaikyti dėl neteisėto valstybės sienos kirtimo jūra, sausuma ar oru iš trečiosios šalies ir kurie nebuv'o grąžinti atgal į tą šalį, judėjimo kontrolę. Šiame registre tvarkomi žmogaus išorės požymių duomenys, gauti asmenis fotografuojant, matuojant bei aprašant jų išorę. Pagal šį apibrėžimą bei šio registro statusą reguliuojančiame Lietuvos Respublikos vidaus reikalų ministro įsakyme pateikiamą tvarkomų duomenų sąrašą Habitoskopinių duomenų registre tvarkomi asmens duomenys, ne-patenkantys į biometrinių asmens duomenų apibrėžtį. Tačiau viešai interneše skelbiame projekto „HDR modernizavimas, panaudojant pažangias asmens veido atpažinimo ir asmens paieškos pagal atpažinimo žymes technologijas“ aprašyme nurodoma, kad „projektu siekiama minėtoms institucijoms sudaryti sąlygas naudojant HDR priemones ne tik gauti asmens atpažinimo duomenis, bet ir patogiai, greitai ir tiksliai nustatyti asmenų, įtariamų padarius nusikalstamą veiką, ar užsieniečių, neteisėtai kirtusių valstybės sieną, taip pat neatpažintų lavonų ir nežinomų bei jėgių asmenų, ar kitų kategorijų identifikuojamų asmenų tapatybę“. Ten pat nurodoma, kad „vykdant projekto veiklas modernizuota HDR Asmens veido biometrinio atpažinimo posistemė, panaudojant pažangias veido biometrinio atpažinimo technologijas, pagerintas asmens veido biometrinio atpažinimo tikslumas, našumas bei patikimumas. Modernizuotos HDR asmens veido biometrinio atpažinimo funkcijos, naudojant didelio tikslumo veido biometrinio atpažinimo programinę įrangą („NeoFace Watch“, gamintojas – NEC korporacija), kuri suteikia galimybę programinės įrangos naudotojams atliliki asmens veido biometrinį atpažinimą (1:1; 1:N) netiesioginiu režimu, naudojant skaitmenines veido nuotraukas, ir asmens veido biometrinį atpažinimą (N:N) tiesioginiu režimu, naudojant realiu laiku veikiančias IP vaizdo kameras. Įsigyta asmens veido biometrinio atpažinimo programinė įranga turi ir specialiai sukurtą programinės įrangos komponentą, skirtą išmaniesiems įrenginiams. Išmaniojo įrenginio „Veido atpažinimo“ aplikacija suteikia galimybę mobiliam asmens veido atpažinimui, tai yra, nufotografuoti asmenį telefonu ir atliliki tokio asmens veido atvaizdo paiešką (atpažinimą) pagal sukauptus veido atvaizdo duomenis HDR duomenų bazėje.“¹⁵⁶

Kitame projekte, apie kurį skelbiama Lietuvos Respublikos policijos departamento interneto svetainėje, taip pat kalbama apie Habitoskopinių duomenų registrui teikia-

¹⁵⁶ Informatikos ir ryšių departamentas. Įgyvendinant Vidaus saugumo fondo lėšomis finansuojamą projektą modernizuotas Habitoskopinių duomenų registratoras – įdiegtos pažangios asmens veido biometrinio atpažinimo technologijos. Prieiga per internetą: <https://ird.lt/lt/naujienos/igyvendinant-vidaus-saugumo-fondo-lesomis-finansuojama-projekta-modernizuotas-habitoskopiniu-duomenu-registras-idiegtos-pazangios-asmens-veido-biometrinio-atpazinimo-technologijos>.

mū veido atvaizdū, skirtū būtent apdorojimui specialia technologija, kad būtū gauti biometriniai duomenys, rinkimo proceso modernizavimą: „Projekto tikslas – sukurti vienodą sistemą, skirtą asmens atpažinimo žymėms ir biometriniam duomenims rinkti ir jiems teikti į Lietuvos Respublikos vidaus reikalų ministerijos habitoskopinių duomenų registrą (toliau – HDR). Igyvendinus Projektą, šalies apskričių vyriausiuose policijos komisariatuose ir areštinėse buvo įsigyta 16 vnt. specializuotų darbo vietų, skirtų asmens atpažinimo žymėms ir biometriniam duomenims rinkti ir jiems teikti į HDR. Atsirado galimybė užfiksuoti nenustatyti asmenų atvaizdus, paimti biometrinius duomenis, taip pat ir kitus su asmeniu susijusio įvykio duomenis, juos apdoroti Policijos areštinėje ir sulaikymo patalpų registre ir perduoti įrašyti į HDR. Sulaikius asmenį, įtariamą padarius nusikaltimą, galima asmens biometrinius duomenis operatyviai sulyginti su HDR esančiais duomenimis – tokiu būdu šie duomenys bus naudojami siekiant greičiau atskleisti nusikalstamas veikas, nustatyti asmens tapatybę, efektyviau atliliki tyrimą, greičiau ir kokybiškiau atliliki kriminalistinius tyrimus, užtikrinti nusikalstamumo prevenciją, viešąją tvarką ir visuomenės saugumą.“¹⁵⁷

Kaip buvo minėta, Habitoshkopinių duomenų registrą reguliuojančiame Vidaus reikalų ministro įsakyme nieko nėra užsiminta apie asmens biometrinį duomenų tvarkymą, šių duomenų saugumo užtikrinimą, nenumatyti tokų duomenų saugojimo terminai, prieigos prie jų ribojimai, kaip to reikalaujama remiantis Asmens duomenų tvarkomu nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymu.

Taip pat pažymėtina, kad informacijoje apie Habitoshkopinių duomenų registro modernizavimo projektą nurodoma, kad projektu yra sukurtos trys naujos integracinių sąsajos: su Integrhuota baudžiamojo proceso informacine sistema (IBPS), Administracinių nusižengimų registru (ANR) ir Lietuvos nacionaline antrosios kartos Šenango informacine sistema (N.SIS)¹⁵⁸. Tačiau minėtame ši registrą reguliuojančiame Vidaus reikalų ministro įsakyme nėra tokias sąsajas įgalinančių nuostatų. Taigi, nėra aišku, kokiu teisiniu pagrindu ir kokiais atvejais bus dalinamasi biometriniais duomenimis tarp Habitoshkopinių duomenų registro ir Administracinių nusižengimų registro.

Lietuvos socialinių mokslų centro Teisės institutas 2022 m. birželio mėnesį oficialiu raštu¹⁵⁹ kreipėsi į Vidaus reikalų ministeriją prašydamas paaiškinti atotrūkį tarp

¹⁵⁷ Lietuvos policija. *Sukurta vienoda asmens atpažinimo žymių ir biometriniių duomenų rinkimo sistema*. Prieiga per internetą: <https://policija.lrv.lt/lit/naujienos/sukurta-vienoda-asmens-atpažinimo-zymiu-ir-biometriniu-duomeniu-rinkimo-sistema>.

¹⁵⁸ Informatikos ir ryšių departamentas.

¹⁵⁹ Lietuvos socialinių mokslų centro 2022 m. birželio 14 d. raštas Nr. 2R-29-(1.11) „Dėl tarnybinės pagalbos teikimo vykdant mokslių tyrimą“.

4. DIRBTINIO INTELEKTO NAUDOJIMO KELIAMOS GRĒSMĖS PRIVATUMUI

teisinio reguliavimo ir pagal viešai skelbiama informaciją vykdomos veiklos (t. y. biometriinių duomenų tvarkymo nesant aiškaus teisinio pagrindo), tačiau atsakymas nebuvo pateiktas.

Taigi, tokia situacija implikuoja, kad teisėsaugos vykdomi asmens duomenų rinkimo ir transformavimo į biometrinius duomenis veiksmai jei ir nėra neteisėti (jei vis dėlto yra teisinis pagrindas, tik jis nėra viešai skelbiamas), tai bet kuriuo atveju tokiai praktikai trūksta skaidrumo. Pirma, Habitoskopinių duomenų registro apraše nėra numatyta galimybė saugoti ar tvarkyti biometrinius duomenis, o remiantis informacija apie šio registro atnaujinimą yra akivaizdu, kad biometriniai duomenys Jame yra saugomi. Antra, Habitoskopinių duomenų registro apraše nenumatytas šiame registre laikomų duomenų susiejimas su Integruota baudžiamojo proceso informacine sistema (IBPS), Administracinių nusižengimų registru (ANR) ir Lietuvos nacionaline antrosios kartos Šengeno informacine sistema (N.SIS), tačiau, pagal skelbiama informaciją apie šio registro atnaujinimą, panašu, kad tokios sąsajos yra įdiegtos.

Apibendrinant darytina išvada, kad dirbtinio intelekto naudojimas tiek privaćia-me, tiek viešajame sektoriuje kelia nemažai ir įvairių grėsmių asmens privatumui ir duomenų apsaugai. Didėjant duomenų kiekiui, techninėms galimybėms rinkti duomenis, galimybėms gretinti duomenis tarpusavyje ir pasitelkus dirbtinį intelektą iš esamų duomenų generuoti naujus duomenis, manipuliuojant daryti poveikį asmenų psichinei neliečiamybei, priimti asmenims didelį poveikį turinčius sprendimus neturint galimybės paaiškinti jų priėmimo argumentų bei logikos, ir atsižvelgiant į tai, kad šios tendencijos tik stiprės – neabejotinai didėja poreikis kuo skubiau imtis teisinių priemonių siekiant ginti asmenų teisę į privatumą ir duomenų apsaugą.

5. DIRBTINIO INTELEKTO TEISINIO REGULIAVIMO PERSPEKTYVOS

Nei Europos Sajungoje, nei Lietuvoje nėra teisės akto, skirto dirbtinio intelekto sistemų naudojimo ir su juo susijusios veiklos reguliavimui. Dirbtinio intelekto veiklą riboja bendrieji teisės aktų reikalavimai, susiję su žmogaus teisių apsauga. Vienas svarbiausių šios srities dokumentų – Bendrasis duomenų apsaugos reglamentas, Duomenų apsaugos teisėsaugos srityje direktyva bei Lietuvoje ją įgyvendinantis Asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojos persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas. Tačiau šie dokumentai nustato tik ribojimus, susijusius su asmens duomenų apsauga, ir tai, kaip apibūdinta anksčiau, nėra pakankama tinkamam asmenų teisės į privatumą ir duomenų apsaugą užtikrinimui naudojant dirbtinį intelektą. Teisės į privatumą užtikrinimą taip pat reguliuoja E-Privatumo direktyva¹⁶⁰ bei Elektroninių ryšių įstatymas^{161, 162}.

Tiesa, Europos Sajungoje yra keli programiniai dokumentai, skirti dirbtiniams intelektui. Vienas pirmųjų svarbių šios srities dokumentų – 2018 metų Europos Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui *Dirbtinis intelektas Europai*¹⁶³, kuriami aptariamas poreikis Europai reaguoti į technologinius pokyčius, susijusius su technologine pažanga ir didėjančiu dirbtinio intelekto plėtojimu ir naujodžiu pasaulyje, Europos Sajungos padėtis konkurencingoje tarptautinėje aplinkoje, siūlomi tolesni veiksmai dėl dirbtinio intelekto kūrimo ir naudojimo Europos Sajungos valstybėse – Europos Sajungos technologinių ir pramoninių pajėgumų stiprinimas ir dirbtinio intelekto diegimas visame ūkyje, pasiruošimas socialiniams ir ekonominiams pokyčiams, susijusiems su dirbtinio intelekto plėtra, tinkamos etinės ir tei-

¹⁶⁰ Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL L 201, 31.7.2002.

¹⁶¹ Lietuvos Respublikos elektroninių ryšių įstatymas (Žin., 2004, Nr. 69-2382).

¹⁶² Atsižvelgiant į tai, kad E-Privatumo direktyva ir Elektroninių ryšių įstatymas yra susiję tik su elektro-ninių ryšių ir priemonių naudojimo, o ne saugotinų objektų (teisės į privatumą ar duomenų) apsaugos taisyklėmis, šioje studijoje šie dokumentai nėra išsamiai analizuojami.

¹⁶³ Europos Komisija, 2018.

sinės sistemos užtikrinimas, jėgų sutelkimas dirbtinio intelekto plėtrai įtraukiant valstybes nares ir t. t. Taip pat Europos Komisija sutarė su valstybėmis narėmis dėl Suderinto plano strategijoms suderinti¹⁶⁴. Komisija taip pat sudarė Aukšto lygio ekspertų grupę, kuri 2019 m. balandžio mėnesį paskelbė Patikimo dirbtinio intelekto etikos gaires¹⁶⁵. 2019 metais Europos Komisija paskelbė komunikatą¹⁶⁶, kuriaame palankiai įvertino septynis pagrindinius reikalavimus, nustatytus Aukšto lygio ekspertų grupės gairėse: žmogiškasis veiksnys ir žmogaus atliekama priežiūra, techninis patvarumas ir saugumas, privatumas ir duomenų valdymas bei skaidrumas, įvairovė, nediskriminavimas ir teisingumas, visuomenės ir aplinkos gerovė, atskaitomybė. 2020 m. Europos Komisija paskelbė naują dokumentą – baltąją knygą „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“¹⁶⁷. Šioje knygoje analizuojamas pramonės ir profesinių rinkų pranašumų išnaudojimas, ateities galimybų išnaudojimas atsižvelgiant į naują duomenų bangą, kompetencijos ekosistema – bendradarbiavimas su valstybėmis narėmis, mokslo ir inovacijų bendruomenės pastangų telkimas, viešojo ir privataus sektoriaus indėlis ir galimybės plėtojant ir naudojant dirbtinį intelektą, esama teisinė bazė, planuojamos Europos Sąjungos dirbtinio intelekto reglamentavimo sistemos aprėptis ir t. t. Šioje baltojoje knygoje nurodyta, kad dirbtinio intelekto kūrėjams ir diegėjams taikomi bendrieji Europos teisės aktai dėl pagrindinių teisių (pvz., duomenų apsaugos, privatumo, nediskriminavimo), vartotojų apsaugos, gaminių saugos ir atsakomybės taisyklės. Vartotojai tikisi tokio pat saugos lygio ir pagarbos jų teisėms, nepriklausomai nuo to, ar produktas arba sistema grindžiamas dirbtiniu intelektu, ar ne. Tačiau dėl tam tikrų dirbtinio intelekto ypatumų (pvz., neskaidrumo) šiuos teisės aktus gali būti sunkiau taikyti ir užtikrinti jų vykdymą. Taip pat pabrėžta, kad tvirta europinė patikimo dirbtinio intelekto reglamentavimo sistema apsaugos visus Europos piliečius ir padės kurti sklandžiai veikiančią vidaus rinką, kad būtų galima toliau plėtoti ir diegti dirbtinį intelektą ir stiprinti Europos pramoninę dirbtinio intelekto bazę.

Taigi, kaip matyti, Europos Sąjungos pirminis tikslas yra lyderiauti pasaulyje kuriant ir naudojant dirbtinį intelektą įvairiuose viešojo ir privataus gyvenimo procesuose. Tačiau buvo pripažinta, kad tam, jog būtų tinkamai apsaugotos žmogaus teisės, esamų teisinių instrumentų nepakanka, ir galiausiai 2021 metais Europos Komisija pateikė Pasiūlymą dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustato-

¹⁶⁴ Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Suderintas dirbtinio intelekto planas. COM(2018) 795.

¹⁶⁵ Europos Komisija. Patikimo dirbtinio intelekto gairės.

¹⁶⁶ Europos Komisija, 2019.

¹⁶⁷ Europos Komisija, 2020.

mos suderintos dirbtinio intelekto taisyklos (dirbtinio intelekto aktas)¹⁶⁸. Šiuo teisės aktu siekiama kelių tikslų:

- užtikrinti, kad Sąjungos rinkai pateikiamas ir naudojamos dirbtinio intelekto sistemos būtų saugios ir derėtų su dabartinių pagrindinės teises ir Sąjungos vertybes reglamentuojančiais teisės aktais;
- užtikrinti teisinį tikrumą, siekiant sudaryti palankesnes sąlygas investicijoms ir inovacijoms dirbtinio intelekto srityje;
- gerinti valdymą ir veiksmingą dabartinių teisės aktų, kuriais reglamentuojaamos pagrindinės teisės ir dirbtinio intelekto sistemoms taikytini saugos reikalavimai, vykdymo užtikrinimą;
- palengvinti bendrosios teisėtų, saugų ir patikimų dirbtinio intelekto prietaikų rinkos plėtrą ir užkirsti kelią rinkos susiskaidymui.

Kaip teigiama šio akto aiškinamajame rašte, siekiant aukščiau nurodytų tikslų, Pasiliūyme pateikiamas subalansuotas ir proporcinges horizontalusis požiūris į dirbtinio intelekto reglamentavimą, apimantis minimalius būtinus reikalavimus, kad būtų pašalinta su dirbtiniu intelektu susijusi rizika ir problemos, nepagrįstai neapribojant ir netrukdomi technologinės plėtros arba kitaip neproporcingai nepadidinant dirbtinio intelekto sprendimų pateikimo rinkai išlaidų. Pasiūlymu nustatoma patikima ir lanksti teisinė sistema. Viena vertus, ji, atsižvelgiant į pagrindinius sprendimus reglamentavimo srityje, išskaitant principais grindžiamus reikalavimus, kuriuos turėtų atitinkti dirbtinio intelekto sistemas, yra išsami ir orientuota į ateitį. Kita vertus, ja nustatoma proporcina reglamentavimo sistema, grindžiama tinkamai apibrėžtu, rizika pagrįstu reglamentavimo metodu, kuriuo nesukuriami nereikalingi apribojimai prekybai, pagal kurį teisinė intervencija pritaikoma prie konkrečių situacijų. Kartu teisinėje sistemoje numatyti lankstūs mechanizmai, kurie sudaro sąlygas ją dinamiškai pritaikyti prie technologinių pokyčių ir naujų situacijų¹⁶⁹.

Kalbant apie Dirbtinio intelekto akte pateikiamus saugiklius dėl teisės į privatumą ir asmens duomenų apsaugos, išskirtinos šios nuostatos:

Pirma, šiame pasiliūyme nustatyta patikima rizikos metodika, kuria remiantis apibrėžiamos didelės rizikos dirbtinio intelekto sistemas, keliančios didelę riziką asmenų sveikatai ir saugai arba pagrindinėms teisėms. Šios dirbtinio intelekto sistemas turės atitinkti patikimam dirbtiniam intelektui taikomą horizontalių privalomų reikalavimų rinkinį ir prieš šias sistemas pateikiant Sąjungos rinkai turės būti atliktos atitinkties

¹⁶⁸ Europos Komisijos Pasiliūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklos (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktais. COM(2021) 206 final.

¹⁶⁹ Dirbtinio intelekto akto aiškinamasis raštas, p. 3.

vertinimo procedūros. Be to, bus sukurta bendra Europos Sąjungos didelės rizikos dirbtinio intelekto sistemų duomenų bazė, kurią tvarkys Komisija, o duomenis jai teiks dirbtinio intelekto sistemų tiekėjai prieš pradedant naudoti šias sistemas. Bet kurie suinteresuoti asmenys galės patikrinti, ar didelės rizikos dirbtinio intelekto sistema atitinka pasiūlyme nustatytus reikalavimus.

Antra, Pasiūlyme pateiktas draudžiamos dirbtinio intelekto naudojimo praktikos sąrašas apima visas dirbtinio intelekto sistemas, kurių naudojimas laikomas nepriimtinu dėl prieštaravimo Sąjungos vertybėms, pavyzdžiu, dirbtinio intelekto sistemos pažeidžiamos pagrindinės teisės.

- Pavyzdžiu, draudžiama praktika, kuri gali turėti reikšmingą potencialą manipuliuoti asmenimis naudojant pasąmonę veikiančius metodus, kurių jie nesuvokia, arba išnaudojant konkrečių pažeidžiamų grupių, pavyzdžiu, vaikų arba neigaliųjų, pažeidžiamumo aspektus, siekiant iš esmės pakeisti jų elgesį taip, kad jie patys ar kitas asmuo patirtų psichologinę arba fizinę žalą. Tačiau atkreipiamas dėmesys, kad draudimas taikomas tik pažeidžiamų grupių atžvilgiu, o kita manipuliavimo arba išnaudojimo praktika, daranti poveikį suaugusiesiems, kurių gali palengvinti dirbtinio intelekto sistemos, gali būti reglamentuojama pagal galiojančius duomenų apsaugos, vartotojų apsaugos ir skaitmeninių paslaugų teisės aktus, kuriais garantuojamas tinkamas fizinių asmenų informavimas ir suteikiama galimybė nuspręsti, kad jiems nebūtų taikomas profiliavimas arba kita poveikį jų elgesiui galinti daryti praktika.
- Draudžiama valdžios institucijoms bendraisiais tikslais vykdysti dirbtiniu intelektu pagrįstą socialinį reitingavimą.
- Draudžiamas tikralaikio (angl. *real-time*) nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešosiose erdvėse teisėsaugos tikslais, išskyrus atvejus, kai taikomos tam tikros ribotos išimtys, t. y. i) tik vykdant tikslinę konkrečių galimų nusikaltimo aukų, iškaitant dingusius vaikus, paiešką; ii) siekiant išvengti konkrečios didelės artėjančios grėsmės fizinių asmenų gyvybei ar fizienei saugai arba teroristinio išpuolio; iii) siekiant išaiškinti apysunkius, sunkius ar labai sunkius nusikaltimus padariusius asmenis, atsižvelgiant į žalos, kuri būtų padaryta nenaudojant tokios sistemos, dydį, tikimybę ir mastą bei sistemos naudojimo pasekmes; taip pat šių priemonių naudojimas turi būti būtinės ir proporcingas. Be to, kiekvienu atskiru atveju privaloma gauti teisminės institucijos arba nepriklausomos administraciniės institucijos leidimą naudoti tokią sistemą (išimtiniais atvejais, kai sistemą naudoti reikia nedelsiant, leidimas gali būti išduotas vėliau)¹⁷⁰⁾.

¹⁷⁰⁾ Pasiūlymo dėl Dirbtinio intelekto akto 5 straipsnis.

Trečia, specialios nuostatos taikomos su manipuliavimo rizika susijusioms sistemos, kurios i) sąveikauja su žmonėmis, ii) naudojamos emocijoms arba asociacijoms su (socialinėmis) kategorijomis nustatyti remiantis biometriniais duomenimis arba iii) kuria turinį, arba juo manipuliuoja (sintetinė sankaita, angl. *deep fake*). Tais atvejais, kai asmenys sąveikauja su dirbtinio intelekto sistema arba jų emocijos ar savybės atpažįstamos automatinėmis priemonėmis, žmonės apie šias aplinkybes turi būti informuojami.

Ketvirta, nustatyti griežti skaidrumo ir informacijos atskleidimo naudotojams reikalavimai, t. y. dirbtinio intelekto sistemų naudotojams privalo būti išduotos išsamios naudojimo instrukcijos. Pabrėžtina, kad instrukcijos išduodamos naudotojams, bet ne asmenims, kurių atžvilgiu taikomos dirbtinio intelekto sistemos (t. y. numatyta pareiga juos informuoti apie dirbtinio intelekto sistemų naudojimą, tačiau nėra išsamiai detalizuota, kiek informacijos turi būti atskleista).

Penkta, nustatytas reikalavimas, kad didelės rizikos dirbtinio intelekto sistemų veikimą galėtų prižiūrėti fiziniai asmenys. Numatyta, kad fiziniai asmenys turi gebeti netaikyti dirbtinio intelekto pateikto rezultato, siekdami išvengti „automatinio šališkumo“.

Šešta, tais atvejais, kai dirbtinio intelekto sistema sąveikauja su fiziniais asmenimis, šie asmenys privalo būti informuojami apie tai, kad sąveikauja su dirbtinio intelekto sistema, nebent tai būtų akivaizdu iš aplinkybių ir naudojimo konteksto. Analogiškai asmenims turi būti pranešta apie emocijų atpažinimo arba biometrinio kategorizavimo sistemų, sintetinių sankaitų (angl. *deep fake*) naudojimą. Tačiau toks reikalavimas netaikomas dirbtinio intelekto sistemoms, kurias pagal teisės aktus leidžiama naudoti siekiant nustatyti nusikalstamas veikas ar užkirsti joms kelią.

Kaip matyti, Pasiūlymu dėl Dirbtinio intelekto akto bent iš dalies siekiama išspressti ankstesniame šios studijos skyriuje iškeltas problemas, susijusias su galimais privatumo ir duomenų apsaugos pažeidimais naudojant dirbtinio intelekto sistemas. Pavyzdžiui, stipriai ribojamos manipuliacijų ir psichinės neliečiamybės pažeidimų galimybės (tiesa, kadangi, kaip minėta, šis Pasiūlymas grindžiamas „lanksčiomis nuostatomis“, siekiant nepaneigti dirbtinio intelekto teikiamos naudos Europos Sąjungai, visuomenei ir atskiriems asmenims, dar kol kas nėra aišku, kaip šios nuostatos bus įgyvendintos praktikoje). Taip pat griežtinamas didelės rizikos dirbtinio intelekto sistemų naudojimas – t. y. jei dirbtinis intelektas gali daryti poveikį žmogaus teisėms ir laisvėms, tokioms sistemoms taikomi griežti skaidrumo, sertifikavimo, priežiūros, žmogiško indėlio ir kt. reikalavimai.

Tačiau ne visi su privatumo ir duomenų apsauga susiję aspektai yra išsprendžiami pateiktu pasiūlymu.

Pavyzdžiui, iš esmės nėra kalbama apie papildomus saugiklius duomenų rinkimo

mastui ir kokybei. Tiesa, tam taikytini skaidrumo reikalavimai, tačiau jie neišsprendžia išskeltų problemų dėl kišimosi į privatų gyvenimą grėsmių, jei duomenys bus agreguoti, atskleisti ar renkami tokios kokybės, kuri akivaizdžiai pažeidžia žmogaus privatumą.

Taip pat atkreiptinas dėmesys į tai, jog Pasiūlyme daromas skirtumas tarp tikralakio ir netikralakio nuotolinio biometrinio tapatybės nustatymo sistemų. Griežtesnės taisyklės taikomos tikralakėms nuotolinio biometrinio tapatybės nustatymo sistemos, tačiau, žvelgiant iš teisės į privatumą ir duomenų apsaugos perspektyvos, kišimasis į privatų gyvenimą yra vienodai galimas tiek tiesiogiai nustatant asmens tapatybę, tiek ir apdorojant jo veido ar kitus biometrinius duomenis vėliau naudojant veido atpažinimo ar kitas biometrinio apdorojimo priemones.

Pažymėtina ir tai, kad Pasiūlyme daroma nemažai išimčių tais atvejais, kai dirbtinio intelekto sistemos yra naudojamos teisėsaugos tikslais. Kiek toks naudojimas kels grėsmę asmens privatumui, priklausys nuo to, kaip šiu sistemų naudojimas bus taikomas praktikoje. Atsižvelgiant į tai, kaip neviešinama informacija Lietuvoje apie asmens biometrinį duomenų naudojimą teisėsaugos darbe, kyla abejonių, ar tokios aptakios ir plačiai interpretuotinos Pasiūlymo nuostatos pakeis dabartinę situaciją.

Pasiūlymas dėl Dirbtinio intelekto akto nesprendžia ir duomenų aggregavimo bei naujų duomenų kūrimo iššūkio. Tiesa, iš dalies tą reguliuoja reikalavimas taikyti žmogišką kontrolę, tačiau tai nepaneigia faktą, kad dirbtinio intelekto sugeneruoti duomenys, ypač privataus pobūdžio duomenys (pvz., iš tam tikrų duomenų visumos dirbtinis intelektas sugeneruoja išvadą, kad asmuo yra neištikimas savo sutuoktinui), gali pažeisti teisę į privatumą.

Galiausiai, Pasiūlyme nesprendžiama problema dėl sprendimų priėmimo aiškumo ir argumentavimo. Tačiau, atsižvelgiant į poreikį užtikrinti asmenų civilines teises, 2022 m. spalio mėnesį Europos Komisija pateikė Pasiūlymą dėl Direktyvos dėl nesutartinės civilinės atsakomybės taikymo dirbtiniams intelektui¹⁷¹. Remiantis šiuo Pasiūlymu dėl direktyvos, asmenims, kurie kreipiasi į teismą dėl sprendimo, priimto pasitelkus dirbtinį intelektą, ir kuriems nėra atskleidžiami priimto sprendimo argumentai ir logika, bus perkelta įrodinėjimo našta kitai ginčo pusei, sudarant galimybes tinkamiai apginti savo teises.

Kaip matyti, planuojamas dirbtinio intelekto reguliavimas Europos Sąjungos lygmeniu pirmiausia yra nukreiptas į galimybes šalinti kliūtis ir sudaryti kuo palankesnės sąlygas dirbtinio intelekto kūrimui ir naudojimui. Tiesa, nustatyta ir pareiga sau-goti žmogaus teises, ypač kalbant apie didelės rizikos dirbtinio intelekto sistemas, t. y. tas sistemas, kuriomis keliama didžiausia grėsmė žmogaus teisių pažeidimams.

¹⁷¹ European Commission. Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence. COM(2022) 496 final.

Tačiau, kaip buvo pastebėta, daugelis žmogaus teises ginančių nuostatų Pasiūlyme dėl Dirbtinio intelekto akto gali būti skirtingai interpretuojamos, be to, jos neatliepia į visus dirbtinio intelekto sistemų naudojimo keliamus iššūkius asmens privatumui. Antra vertus, nereikia pamiršti, kad ne tik dirbtinio intelekto kūrimo ir naudojimo plėtra nestovi vietoje – ir teisėkūra yra nuolat tobulinama ir keičiama, ir tą patvirtina vienas pastarujų Europos Komisijos pasiūlymų dėl Direktyvos dėl dirbtinio intelekto sistemų civilinės atsakomybės taisyklių.

1. Dirbtinis intelektas yra vienas svarbiausių pastarujų metų technologinių sprendimų, leidžiančių žmonijai iš esmės keisti įprastas darbo rutinas, spartinti gamybą, gyventojų aptarnavimą, viešujų paslaugų teikimą, optimizuoti viešąjį ir privatų gyvenimą. Sparti dirbtinio intelekto technologijų plėtra rodo, kad dirbtinio intelekto kūrimas ir naudojimas nuolat kinta, kuriami ir praktikoje naudojami nauji modeliai, dirbtinis intelektas bus pritaikomas vis įvairesnėse srityse. Dirbtinis intelektas didina tiek atskirų valstybių, tiek Europos Sąjungos konkurencingumą tarptautiniu lygmeniu, dėl to politiniu lygmeniu laikomasi požiūrio, jog teisė turi prisitaikyti prie technologinių naujovių ir nustatyti saugiklius, kad žmogaus teisės jas naudojant nebūtų pažeidžiamos, o ne stabdyti technologinį progresą.
2. Nepaisant dirbtinio intelekto pažangos teikiamas naudos, šių sistemų naudojimas turi ir šalutinį poveikį – kelia įvairaus pobūdžio ir įvairios prigimties grėsmių tiek tam tikroms visuomenės grupėms, tiek individualiems asmenims. Ypač tai pasakytina apie tokius atvejus, kai dirbtinis intelektas pats generuoja sprendimus ir išvadas tik iš duomenų, be jokių žmogaus teikiamų instrukcijų. Tokia situacija patraukė teisės į privatumą ir asmens duomenų apsaugos institucijų dėmesį visame pasaulyje ir taip pat privertė žmogaus teisių gynėjus ir politikus reaguoti ir ieškoti teisinių sprendimų.
3. Dirbtinio intelekto sistemų naudojimui keliami teisiniai reikalavimai dėl teisės į privatų gyvenimą užtikrinimo ir asmens duomenų apsaugos apima ir reikalavimą taikyti proporcinguo ir būtinumo testą, taip pat atitinkti duomenų mažinimo, duomenų tikslumo, saugojimo ribojimo, duomenų apsaugos ir atskaitingumo reikalavimus. Lietuvos Respublikos Konstitucinis Teismas taip pat yra pateikęs taisykles, kurių turi būti laikomasi naudojant dirbtinio intelekto sistemas – užtikrinant privataus gyvenimo apsaugą būtina atsižvelgti į visuomenės raidą bei mokslo ir technologijų pažangą; asmuo turi žinoti (iš anksto ar bent jau *post factum*) apie jo atžvilgiu naudotą asmens duomenų rinkimą; taikant bet kokią priemonę, kuria ribojama teisė į privatumą, turi būti įvertinama, ar negalima tų pačių tikslų pasiekti neįsiterpiant į privatų žmogaus, šeimos gyvenimą ir neapribojant žmogaus teisės į privatumą; teisė į privatumą apima ir teisę į psichinį neliečiamumą. Vadinas, pasitel-

- kus dirbtines technologijas kuriamos manipuliacinės priemonės (pvz., skatinimas daugiau pirkti tam tikrų produktų) yra susijusios su teisės į privatumą pažeidimu.
4. Nepaisant to, kad prekių ir paslaugų teikimui naudojant dirbtinio intelekto sistemas keliami tie patys reikalavimai užtikrinti žmogaus teises, kaip ir teikiant bet kokią kitas prekes ir paslaugas, tačiau dėl dirbtinio intelekto sistemų išskirtinumo atsiranda naujų iššūkių, kuriems trūksta teisinio reguliavimo – pavyzdžiui, dėl nuolatinės technologinės pažangos gerinant duomenų kokybę kyla vis didesnė grėsmė, kad renkami duomenys turės informacijos apie privatų asmens gyvenimą; pasitelkus dirbtinių intelektą asmens duomenys renkami vis iš įvairesnių šaltinių, tuo sudarant galimybes gauti tokį duomenų rinkinį, kuris savaime pažeis žmogaus teisę į privatumą, ir dar daugiau – dirbtinis intelektas tam tikrais atvejais peržengia žmogaus gebėjimų ribas (pvz., geba iš anksto diagnozuoti ligas, kai to dar niekas nepastebi). Be to, didėjant duomenų kiekiui, techninėms galimybėms rinkti duomenis, galimybėms gretinti duomenis tarpusavyje ir pasitelkus dirbtinių intelektą iš esamų duomenų generuoti naujus duomenis, manipuliujant daryti poveikį asmenų psichinei neliečiamybei, priimti asmenims didelį poveikį turinčius sprendimus neturint galimybės paaiškinti jų priėmimo argumentų bei logikos ir atsižvelgiant į tai, kad šios tendencijos tik stiprės – neabejotinai didėja poreikis kuo skubiau imtis teisinių priemonių siekiant ginti asmenų teisę į privatumą ir duomenų apsaugą.
 5. Dirbtinio intelekto naudojimo Lietuvoje teisinis reguliavimas, ypač atsižvelgiant į keliamas grėsmes žmogaus privatumui ir duomenų apsaugai, nėra pakankamas. Pavyzdžiui, Lietuvos Habitoskopinių duomenų registre naudojant veido atpažinimo technologijas nėra pakankamas reguliavimas tam, kad būtų užtikrintas biometrių duomenų tvarkymo reikalavimų laikymasis, taip pat stinga aiškaus reguliavimo, kaip duomenys perduodami iš vienos duomenų bazės į kitą, ir pan. Tiesa, atsižvelgiant į tai, kad Europos Sajungoje ketinama priimti Dirbtinio intelekto aktą, kuris būtų taikomas visose valstybėse narėse, šiuo metu imtis reguliacinės iniciatyvos nacionaliniu lygmeniu, tikėtina, būtų neefektyvu. Tačiau net ir nesant nuoseklaus ir visa apimančio dirbtinio intelekto reguliavimo Lietuvoje, būtina užtikrinti, kad, taikant įvairias priemones, susijusias su dirbtinio intelekto naudojimu, nebūtų pažeistos žmogaus teisės, ypač teisę į privatumą ir asmens duomenų apsaugą.
 6. Planuojamas dirbtinio intelekto reguliavimas Europos Sajungos lygmeniu pirmiausia yra nukreiptas į galimybes šalinti kliūtis ir sudaryti kuo palankesnes sąlygas dirbtiniams intelektui kurti ir naudoti. Tiesa, nustatyta ir pareiga saugoti žmogaus teises, ypač kalbant apie didelės rizikos dirbtinio intelekto sistemas, t. y. tas sistemos, kuriomis keliamas didžiausia grėsmė žmogaus teisių pažeidimams. Tačiau daugelis žmogaus teises ginančių nuostatų Europos Komisijos Pasiūlyme dėl

Dirbtinio intelekto akto gali būti skirtingai interpretuojamos, be to, jos neatliepia į visus dirbtinio intelekto sistemų naudojimo keliamus iššūkius asmens privatumui. Pavyzdžiu i, Pasiūlyme dėl Dirbtinio intelekto akto nesprendžiamas klausimas dėl privačių duomenų rinkimo apimties (dėl rizikų, kad šie duomenys bus panaudoti neteisėtai dėl tyčinių veiksmų ar dėl technologinių klaidų), dėl renkamų duomenų kokybės, o tai gali būti susiję su asmens privatumo pažeidimu; dėl asmens duomenų rinkimo ir vėlesnio jų apdorojimo specialia technika gaunant biometrinius asmens duomenis; dėl duomenų aggregavimo ir naujų duomenų kūrimo. Tiesa, nors Pasiūlyme dėl Dirbtinio intelekto akto nėra kalbama apie pasekmes, kurias sukuria dirbtinio intelekto sistemų priimamų sprendimų nepaaiškinamus, Europos Komisija pateikė Pasiūlymą dėl direktyvos, kuria būtų reguliuojami šie klausimai ir užtikrinama asmenų, nukentėjusių dėl dirbtinio intelekto sistemų priimtų sprendimų, apsauga įrodinėjant savo teises.

LITERATŪRA

Teisės aktai, teisės aktų projektai ir programiniai dokumentai

European Commission. Proposal for a Directive on adapting non contractual civil liability rules to artificial intelligence. COM(2022) 496 final.

Europos Komisija. Baltoji knyga. *Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą*. COM(2020) 65 final.

Europos Komisija. *Patikimo dirbtinio intelekto gairės*. Prieiga per internetą: <https://op.europa.eu/lt/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.

Europos Komisijos komunikatas „Europos žaliasis kursas“. COM(2019) 640 final.

Europos Komisijos Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiamai tam tikri Sąjungos teisėkūros procedūra priimti aktai. COM(2021) 206 final.

Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL L 201, 31.7.2002.

Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119/1.

Europos Sąjungos pagrindinių teisių chartija. OL C 202/389.

Europos žmogaus teisių konvencija. Prieiga per internetą: https://www.echr.coe.int/documents/convention_lit.pdf.

Kaišiadorių rajono savivaldybės tarybos įsakymas „Dėl Kaišiadorių rajono savivaldybės teritorijoje įrengtų vaizdo stebėjimo kamerų ir jų fiksuarotų duomenų naudojimo tvarkos aprašo patvirtinimo“. *Teisės aktų registras*, 2022, Nr. 13200.

Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui *Dirbtinis intelektas Europai*. COM/2018/237 final.

Komisijos komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Suderintas dirbtinio intelekto planas. COM(2018) 795.

Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Pasitikėjimo įžmogų orientuotu dirbtiniu intelektu didinimas. COM(2019) 168 final.

Lietuvos Respublikos administracinių nusizengimų kodeksas. *Teisės aktų registratoras*, 2015, Nr. 11216.

Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojos persekiojimo už jas, bausmių vykdymo arba nacionalinio sau-gumo ar gynybostikslais, teisinės apsaugos įstatymas. *Valstybės žinios*, 2011, Nr. 52-2511.

Lietuvos Respublikos asmens tapatybės kortelės ir paso įstatymas. *Teisės aktų registratoras*, 2014, Nr. 21281.

Lietuvos Respublikos baudžiamojos proceso kodeksas. *Valstybės žinios*, 2002, Nr. 37-1341.

Lietuvos Respublikos bausmių vykdymo kodeksas. *Valstybės žinios*, 2002, Nr. 73-3084.

Lietuvos Respublikos civilinis kodeksas. *Valstybės žinios*, 2000, Nr. 74-2262.

Lietuvos Respublikos ekonomikos ir inovacijų ministerija. Kurk Lietuvai. *Lietuvos dirbtinio intelekto strategija*. Prieiga per internetą: [https://eimin.lrv.lt/uploads/eimin/documents/_files/DI_strategija_LT\(1\).pdf](https://eimin.lrv.lt/uploads/eimin/documents/_files/DI_strategija_LT(1).pdf).

Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004, Nr. 69-2382.

Lietuvos Respublikos finansinių nusikaltimų tyrimo tarnybos įstatymas. *Valstybės žinios* 2002, Nr. 33-1250.

Lietuvos Respublikos įstatymas dėl užsieniečių teisinės padėties. *Valstybės žinios*, 2004-04-30, Nr. 73-2539.

Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, Nr. 33-1014.

Lietuvos Respublikos kriminalinės žvalgybos įstatymas. *Valstybės žinios*, 2012-10-20, Nr. 122-6093.

Lietuvos Respublikos policijos įstatymas. *Valstybės žinios*, 2000, Nr. 90-2777.

Lietuvos Respublikos prokuratūros įstatymas. *Valstybės žinios*, 1994, Nr. 81-1514.

Lietuvos Respublikos specialiųjų tyrimų tarnybos įstatymas. *Valstybės žinios*, 2000, Nr. 41-1162.

Lietuvos Respublikos tarnybinio paso įstatymas. *Valstybės žinios*, 2000, Nr. 7-178.

Lietuvos Respublikos vidaus reikalų ministro 2013 m. gegužės 21 d. įsakymas Nr. 1V-440 dėl Arešto ar terminuoto laisvės atėmimo bausmę atlikusių asmenų atpažinimo žymių žinybinio registro reorganizavimo į Habitoskopinių duomenų registrą.

Lietuvos Respublikos vidaus reikalų ministro įsakymas „Dėl motorinių transporto priemonių vairuotojo pažymėjimų išdavimo taisyklių patvirtinimo“. *Valstybės žinios*, 2008, Nr. 106-4060.

Lietuvos Respublikos vienos savivaldos įstatymas. *Valstybės žinios*, 1994, Nr. 55-1049.

Lietuvos Respublikos žvalgybos įstatymas. *Valstybės žinios*, 2000, Nr. 64-1931.

Šiaulių miesto savivaldybės tarybos įsakymas „Dėl Šiaulių miesto savivaldybės teritorijoje įrengtų vaizdo stebėjimo kamerų ir jų fiksuočių duomenų rinkimo ir naudojimo taisyklių patvirtinimo“. *Teisės aktų registratoras*, 2020, Nr. 10216.

Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamą 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 2008/977/TVR (Teisėsaugos direktyva). OL, L 119/89.

Tauragės rajono savivaldybės tarybos įsakymas „Dėl Tauragės rajono savivaldybės viešosiose erdvėse įrengtų vaizdo stebėjimo kamerų ir jų fiksuotų duomenų naudojimo tvarkos aprašo patvirtinimo“. *Teisės aktų registras*, 2022, Nr. 7557.

Teismų praktika

Europos Žmogaus Teisių Teismo sprendimas *Gaughan prieš Jungtinę Karalystę*. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-12731>.

Europos Žmogaus Teisių Teismo sprendimas *Liberty ir kiti prieš Jungtinę Karalystę*. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-1980>.

Europos Žmogaus Teisių Teismo sprendimas *López Ribalda ir kiti prieš Ispaniją*. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=002-12630>.

Europos Žmogaus Teisių Teismo sprendimas *Szabó ir Vissy prieš Vengriją*. Prieiga per internetą: https://hudoc.echr.coe.int/app/conversion/docx/pdf?library=ECHR&id=001_160020&filename=CASE%20OF%20SZAB%C3%93%20AND%20VISSY%20v.%20HUNGARY.pdf.

Europos Žmogaus Teisių Teismo sprendimas *Weber ir Saravia prieš Vokietiją*. Prieiga per internetą: <https://hudoc.echr.coe.int/fre?i=001-76586>.

Judgment of The Hague District Court of 5 February 2020, case number C/09/550982, ECLI:NL:RBDHA:2020:865.

Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2000 m. gegužės 8 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2002 m. rugsėjo 19 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2002 m. spalio 23 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2004 m. gruodžio 29 d. nutarimas.

Lietuvos Respublikos Konstitucinio Teismo 2017 m. gruodžio 19 d. išvada.

Lietuvos Respublikos Konstitucinio Teismo 2019 m. balandžio 18 d. nutarimas.

Lietuvos Aukščiausiojo Teismo civilinė byla E3K-3-472-916/2017.

Vilniaus apygardos administraciniu teismo 2022 m. gegužės 12 d. administraciniu bylu Nr. eI3-839-809/2022.

Mokslinė literatūra

- Acquisti, A. Privacy and security of personal information: Economic incentives and technological solutions. In: Camp, J., Lewis, R. (eds.). *The Economics of Information Security*. Kluwer, Dordrecht, 2004.
- Buolamwini, J., Gebru, T. Proceedings of the 1st Conference on Fairness, Accountability and Transparency. *PMLR*, 2018, No. 81.
- Danielson, P. Video surveillance for the rest of us: Proliferation, privacy, and ethics education. *International Symposium on Technology and Society*, 6–8 June 2002.
- Davenport, T., Fitts, J. AI Can Help Companies Tap New Sources of Data for Analytics. *Harvard Business Review*, 2021 March 19. Prieiga per internetą: <https://hbr.org/2021/03-ai-can-help-companies-tap-new-sources-of-data-for-analytics>.
- Fussey, P., Murray, D. *Independent Report on the London Metropolitan Police Service's Trial of Live Facial Recognition Technology*. University of Essex, Human Rights Centre, July 2019.
- Goldenfein, J. Algorithmic Transparency and Decision-Making Accountability: Thoughts for buying machine learning algorithms. In: Office of the Victorian Information Commissioner (ed). *Closer to the Machine: Technical, Social, and Legal aspects of AI*, 2019. Prieiga per internetą: <https://ssrn.com/abstract=3445873>.
- Griciūnas, P. Už jūsų ir mūsų laisvę. *IQLIFE*, 2021-01-13. Prieiga per internetą: <https://zurnalas.iqlife.lt/advokatas/pries-jusu-ir-musu-laisve/216478>.
- Griciūnas, P. Pasikinkius „Pegasą“: elektroninių sekimo priemonių mitai ir tikrovė. *IQLIFE*, 2022-01-18. Prieiga per internetą: <https://zurnalas.iqlife.lt/advokatas/pasikinkius-pegasas-elektroniniu-sekimo-priemoniu-mitai-ir-tikrove/243188>.
- Hökby, S., Hadlaczky, G., Westerlund, J., Wasserman, D., Balazs, J., Germanavicius, A., Machín, N., Meszaros, G., Sarchiapone, M., Värnik, A., Varnik, P., Westerlund, M., Carl, V. Are Mental Health Effects of Internet Use Attributable to the Web-Based Content or Perceived Consequences of Usage? A Longitudinal Study of European Adolescents. *JMIR Ment Health*, 2016, No 3(3).
- Humerick, M. Taking AI personally: how the EU must learn to balance the interests of personal data privacy & artificial intelligence. *Santa Clara High Tech. LJ*, 2008, Vol. 34, Issue 4.
- Jurčys, P. Asmeninių duomenų nuosavybė. *Teisė.Pro*, 2020-08-01. Prieiga per internetą: <https://www.teise.pro/index.php/2020/08/11/p-jurcys-asmeniniu-duomenu-nuosavybe/>.
- Kak, A. *Regulating Biometrics. Global Approaches and Urgent Questions*. AI Now Institute, September 1 2020. Prieiga per internetą: <https://ainowinstitute.org/regulatingbiometrics.html>.
- Kalpokas, I. Dirbtinio intelekto poveikis žmogaus teisėms nėra išimtis. *VDU.lt*, 2021-12-01. Prieiga per internetą: <https://www.vdu.lt/lt/dirbtinio-intelekto-poveikis-zmogaus-teisems-nera-isimtis/>.

- Learned-Miller, E., Ordóñez, V., Morgenstern, J., Buolamwini, J. *Facial Recognition Technologies in the Wild: A Call for a Federal Office*. Prieiga per internetą: <https://www.semanticscholar.org/paper/FACIAL-RECOGNITION-TECHNOLOGIES-IN-THE-WILD%3A-A-CALL-Learned-Miller-Ordonez/0e637f1cb06f7dd58ed8ad2038fb7bae1e7b45c2>.
- Legal Analysis for TELEFI project Towards the European Level Exchange of Facial Images. Prieiga per internetą: https://www.telefi-project.eu/sites/default/files/TELEFI_LegalAnalysis.pdf.
- Li S. Z., Jain, A. K. *Handbook of Face Recognition*. Springer, 2011.
- Mantelero, A. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*, 2018, Vol. 34, issue 4.
- Montag, L., Mcleod, R., Lara Mets, L., Gauld, M., Rodger, F., Pełka, M. *The Rise and Rise of Biometric Mass Surveillance in EU*. Prieiga per internetą: https://edri.org/wp-content/uploads/2021/07/The-Rise-and-Rise-of-Biometric-Mass-Surveillance-in-the-EU_Dutch-Summary.pdf.
- Pipeda, C. 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation Against FacialRecognition Technology. *Canadian Journal of Law and Technology*. 2020, June.
- Riehm, K. E., Feder, K. A., Tormohlen, K. N., et al. Associations Between Time Spent Using Social Media and Internalizing and Externalizing Problems Among US Youth. *Jama Psychiatry*, 2019, 76(12).
- Rodrigues, R. Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 2020, Vol. 4.
- Stahl, B. C., Wright, D. Ethics and privacy in AI and big data: Implementing responsible research and innovation. *IEEE Security & Privacy*, 2018, Vol. 16, Issue 3.
- Tolan, S., Miron, M., Gomez, E., Castillo, C. *Why Machine Learning May Lead to Unfairness Evidence from Risk Assessment for Juvenile Justice in Catalonia*. Best Paper Award, International Conference on AI and Law, 2019.
- Ubaldi, B., Le Fevre, E. M., Petrucci, E., Marchionni, P., Biancalana, C., Hiltunen, N., Intraavia, D. M., Yang, C. State of the art in the use of emerging technologies in the public sector. *OECD Working Papers on Public Governance*, 2019, No. 31. OECD Publishing, Paris.
- Viechnicki, P., Eggers, W. D. *How much time and money can AI save government? Cognitive technologies could free up hundreds of millions of public sector worker hours*. Deloitte University Press, 2018. Prieiga per internetą: https://www2.deloitte.com/content/dam/insights/us/articles/3834_How-much-time-and-money-can-AI-save-government/DUP -How-much-time-and-money-can-AI-save-government.pdf.
- Wachter, S., Mittelstadt, B., Floridi, L. Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. *International Data Privacy Law*, 2017, Vol. 7, No. 2.

Wilson, D. Algorithmic patrol: the futures of predictive policing. In: A. Završnik (ed.). *Big Data, Crime and Social Control*. Routledge, London and New York, 2017.

Kiti šaltiniai

Amnesty International, Trapped in the Matrix: Secrecy, Stigma and Bias in the Met's Gang Database. May 2018.

AskeyGeek. Companies using Robotic Process Automation. Prieiga per internetą: <https://www.askeygeek.com/companies-using-robotic-process-automation/>.

Clearview AI principles. Prieiga per internetą: <https://www.clearview.ai/principles>.

Commission's report on Saving Lives: Boosting Car Safety in the EU (COM(2016) 0787 final).

CompTIA. Using AI in Business: Examples of Artificial Intelligence Application in Business. Prieiga per internetą: <https://connect.comptia.org/blog/using-ai-in-business>.

Council of Europe. Algorithms and Human Rights. DGI, 2018. Prieiga per internetą: <https://rm.coe.int/algorithms-and-human-rights-en-rev/16807956b5>.

Deloitte US. The digital citizen, 2019. Prieiga per internetą: <<https://tinyurl.com/ykqd76qc>>.

Doffman, Z. Hong Kong Exposes Both Sides Of China's Relentless Facial Recognition Machine. *Forbes*. Prieiga per internetą: <https://www.forbes.com/sites/zakdoffman/2019/08/26/hong-kong-exposes-both-sides-of-chinas-relentless-facial-recognition-machine/?sh=302bee6442b7>.

European Commission/Deloitte. Opportunities and Challenges for the Use of Artificial Intelligence in Border Control, Migration and Security. Volume 2: Addendum, 2018.

Prieiga per internetą: <https://op.europa.eu/en/publication-detail/-/publication/69f33ff7-a156-11ea-9d2d-01aa75ed71a1/language-en>.

European Parliament. Artificial Intelligence and Law Enforcement. Impact on Fundamental Rights. Prieiga per internetą: [https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU\(2020\)656295](https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2020)656295).

European Parliament. Artificial Intelligence in policing: safeguards needed against mass surveillance. Prieiga per internetą: <https://www.europarl.europa.eu/news/en/press-room/20210624IPR06917/artificial-intelligence-in-policing-safeguards-needed-against-mass-surveillance>.

European Union Agency for Fundamental Rights. Facial recognition technology: fundamental rights considerations in the context of law enforcement. Prieiga per internetą: <https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law>.

Expert Committee on Human Rights Dimensions of Automated Data Processing and Different Forms of Artificial Intelligence (MSI-AUT), Responsibility and AI: A study of the implications of advanced digital technologies (including AI systems) for the concept of

responsibility within a human rights framework (Rapporteur: Karen Yeung), DGI(2019)05, Council of Europe, September 2019.

Forbes, 7 Amazing Examples Of Computer And Machine Vision In Practice, 2019. Prieiga per internetą: <https://tinyurl.com/w2mj5vv>.

Forbes. 10 Ways AI Is Improving Manufacturing in 2020. Prieiga per internetą: <https://www.forbes.com/sites/louiscolumbus/2020/05/18/10-ways-ai-is-improving-manufacturing-in-2020/?sh=3bebcd5f1e85>.

FRA, Council of Europe and EDPS. *Handbook on European data protection law*. Luxembourg, Publications Office, June 2018.

Hay, C. Review: ‘Coded Bias,’ starring Joy Buolamwini, Cathy O’Neil, Meredith Broussard, Silkie Carlo, Ravi Naik, Zeynep Tufekci and Amy Webb. Prieiga per internetą: <https://culturemixonline.com/tag/daniel-santos/#:~:text=%E2%80%9CCoded%20Bias%E2%80%9D%20includes%20an%20interview%20with%20Daniel%20Santos%C,that%20was%20stitled%20out%20of%20court%20in%202017>.

Informatikos ir ryšių departamentas. Igyvendinant Vidaus saugumo fondo lėšomis finansuojamą projektą modernizuotas Habitoskopinių duomenų registras – įdiegtos pažangios asmens veido biometrinio atpažinimo technologijos. Prieiga per internetą: <https://ird.lt/-lt/naujienos/igyvendinant-vidaus-saugumo-fondo-lesomis-finansuoja-mprojekta-modernizuotas-habitoskopiniu-duomenu-registras-idiegtos-pazangios-asmens-veido-biometrinio-atpazinimo-technologijos>.

Kozyrkov, C. *What is Bias?* Prieiga per internetą: <https://towardsdatascience.com/what-is-a-bias-6606a3bcb814>.

Lietuvos policija. *Sukurta vienoda asmens atpažinimo žymių ir biometrinių duomenų rinkimo sistema*. Prieiga per internetą: <https://policija.lrv.lt/lt/naujienos/sukurta-vienoda-asmens-atpazinimo-zymiu-ir-biometriniu-duomenu-rinkimo-sistema>.

Lietuvos socialinių mokslų centro 2022 m. birželio 14 d. raštas Nr. 2R-29-(1.11) „Dėl tarnybinių pagalbos teikimo vykdant mokslinį tyrimą“.

Medical News Today. Artificial intelligence better than humans at spotting lung cancer. Prieiga per internetą: www.medicalnewstoday.com/articles/325223.php.

Medium, Expert Systems and Applied Artificial Intelligence, 2018. Prieiga per internetą: <https://tinyurl.com/y6demyg>.

OECD Working Papers on Public Governance. Hello, World. Artificial intelligence and its use in the public sector, 2019. Prieiga per internetą: https://www.oecd-ilibrary.org/doc_server/726fd39d-en.pdf?expires=1666023983&id=id&accname=guest&checksum=2B06-78AFDEB937C7A5B42575C7C96F44.

OHCHR. The Right to Privacy in the Digital Age. 3 August 2018, A/HRC/39/29. Prieiga per internetą: <https://undocs.org/A/HRC/39/29>.

Olivia Solon & Cyrus Farivar. Millions of People Uploaded Photos to the Ever App. Then the Company Used Them to Develop FacialRecognition Tools” NBC News, 9 May 2019. Prieiga per internetą: www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371.

Olivia Solon. Facial Recognition’s ‘Dirty Little Secret’: Millions Of Online Photos Scrapped Without Consent. NBC News, 12 March 2019. Prieiga per internetą: <http://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921>.

Partnership for Public Service/IBM Center for the Business of Government. The Future Has Begun. Washington, DC, 2018. Prieiga per internetą: <https://ourpublicservice.org/publications/the-future-has-begun-using-artificial-intelligence-to-transform-government/>.

Privacy International, The SyRI case: a landmark ruling for benefits claimants around the world. Prieiga per internetą: <https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world>.

Smart Data Collective. How Netflix Is Using Artificial Intelligence And Big Data To Drive Business Performance. Prieiga per internetą: <https://www.smartdatacollective.com/how-netflix-is-using-artificial-intelligence-and-big-data-to-drive-business-performance/>.

Stanford news. New Stanford research finds computers are better judges of personality than friends and family. Prieiga per internetą: <http://news.stanford.edu/2015/01/12/personality-computer-knows-011215/>.

Stanford’s robotics legacy. Prieiga per internetą: <https://news.stanford.edu/2019/01/16/stanfords-robotics-legacy/>.

Stockfish 15. Prieiga per internetą: <https://stockfishchess.org/>.

TechGig. Here’s how Amazon is using AI to improve customer support. Prieiga per internetą: <https://content.techgig.com/heres-how-amazon-is-using-ai-to-improve-customer-support/articleshow/74381649.cms>.

The New York Times. In Hong Kong Protests, Faces Become Weapons. Prieiga per internetą: <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html>.

UN Human Rights Committee, draft General Comment No. 37 [Article 21: right of peaceful assembly], draft prepared by the Rapporteur, Christof Heyns, 2019. Prieiga per internetą: <https://www.ohchr.org/en/calls-for-input/call-comment-no-37-article-21-international-covenant-civil-and-political-rights>.

Vilniaus universiteto Medicinos fakulteto informacija. Prieiga per internetą: https://www.mf.vu.lt/images/Remiantis_Vilniaus_universiteto_Medicinos_fakulteto_tarybos_2021.pdf.

Wikipedia. *Jeopardy!* Prieiga per internetą: <https://en.wikipedia.org/wiki/Jeopardy!>.

Wikipedia. *Nearest neighbour algorithm*. Prieiga per internetą: https://en.wikipedia.org/wiki/Nearest_neighbour_algorithm.

SUMMARY

RIGHT TO PRIVACY, PERSONAL DATA PROTECTION AND ARTIFICIAL INTELLIGENCE: CHALLENGES OF LEGAL REGULATION IN LITHUANIA AND EUROPE

Artificial intelligence in public life is being used more and more often and in more and more diverse areas - ensuring public safety, conducting traffic surveillance, collecting data for various public sector reports, marketing purposes, dating portals, etc. Artificial intelligence has already become an important part of our lives. As one of the European Commission points out in its Communicate on artificial intelligence of 2018, the artificial intelligence is no longer science fiction but a reality, acting as a virtual personal assistant to organize the work day, to travel in a self-driving vehicle and to suggest songs or restaurants we might like. Artificial intelligence not only makes our lives easier, but also helps to solve some of the world's biggest challenges: from treating chronic diseases or reducing traffic accident mortality, since about 90 percent road accidents occur due to human error to combating climate change or anticipating cyber security threats.

The primary goal of the European Union is to lead the world in the development and use of artificial intelligence in various processes of public and private life. From the policy documents adopted at the level of the European Union, it is clear that the European Union intends to compete with other regions of the world in the development and use of artificial intelligence systems, and is making significant intellectual, economic and strategic efforts to this end. However, the development and usage of artificial intelligence calls for ensuring that rights of individuals, first of all, the right to private life and personal data, are protected.

Taking into account the scope of the use of artificial intelligence and their development, this study aims to reveal the challenges of the legal regulation of Lithuania and the European Union regarding the use of artificial intelligence in various fields, related to threats to human rights, and primarily to the right to privacy, and to discuss the areas of legal regulation which still needs to be improved.