MYKOLO ROMERIO UNIVERSITETO

VIEŠOJO SAUGUMO AKADEMIJA

PAULIUS GRYBAS

TEISĖ IR IKITEISMINIS TYRIMAS

DIRBTINIO INTELEKTO NAUDOJIMO KELIAMOS GRĖSMĖS ASMENS TEISEI Į PRIVATUMĄ

Magistro baigiamasis darbas

Vadovas: Doc.Dr. E.Štareikė

(mokslinis laipsnis, pedagoginis vardas, vardo pirma raidė, pavardė)

… … … … … … … … … … …

(parašas)

Darbo autorius: P. Grybas

(vardo pirma raidė, pavardė)

… … … … … … … … … … …

(parašas)

Kaunas, 2025

ĮVADAS

SANTRUMPŲ SĄRAŠAS

BDAR – Bendrasis duomenų apsaugos reglamentas

CA – Cambridge Analytica įmonė

DI – Dirbtinis intelektas

ES – Europos Sąjunga

EDAV - Europos duomenų apsaugos valdyba

ĮVADAS

Pagrindiniai pokyčiai informacinių technologijų laikotarpyje, dirbtinio intelekto kontekste, pradėjo formuotis ir atsiskleisti jau apie 2010-2012 metus. Vienas ryškiausių tokių pavyzdžių yra „AlexNet“ – giliojo mokymosi (anglų k. *deep learning)* modelis. 2012 metais vykusiame kasmetiniame „ImageNet“ konkurse „AlexNet“ parodė neįtikėtinus vaizdų atpažinimo rezultatus[1], kuomet buvę klaidų rodikliai, apie 26 % , buvo pagerinti iki 15,3 %. Nors toks proveržis dirbtinio intelekto srityje atvėrė naujas giliojo mokymosi taikymo įvairiose srityse galimybes, tuo metu dirbtinis intelektas dar nebuvo plačiai prieinamas kasdieniniam naudojimui kiekvienam šiuolaikiniam žmogui.

Vis dėlto, per paskutiniuosius dešimt metų, sparčiai vystant informacinių ir dirbtinio intelekto technologijas buvo sukurti modeliai, tokie kaip GPT-3, BERT, Transformer, kurie suteikė naują pagreitį dirbtiniam intelektui. Per paskutiniuosius metus dirbtinis intelektas stipriai pradėjo veikti šiandieninės visuomenės kasdienybėje. Šiandien jis naudojamas įvairiausiose srityse, pavyzdžiui – mobilieji telefonai, kuriuose veikia balsu valdomi asistentai, veido atpažinimo funkcijos, namų išmaniuosiuose įrenginiuose, miesto stebėjimo sistemose, sveikatos priežiūros sistemoje, socialiniuose tinkluose ar finansų srityje. Pavyzdžių, kuriais galima pagrįsti dirbtinio intelekto veikimą mūsų kasdienybėje, yra daugybė. Mes dažnai galime nesusimąstyti, kad kasdien susiduriame su dirbtinio intelekto sprendimais, kurie gali daryti įtaką mūsų privatumui, kas ir parodo šio darbo **temos aktualumą**. Šios **temos naujumą** galima pagrįsti jau anksčiau paminėtuose faktuose, kad dirbtinio intelekto technologija, tik pastaraisiais metais, pradėjo sparčiai vystytis, o jo panaudojimo galimybės plečiasi nuolat. Toks spartus plėtimasis kartu sukuria ir naujas grėsmes asmens teisei į privatumą, su kuriomis ankstesnės kartos dar nebuvo susidūrusios. Ši tema pasirinktina ne tik dėl jos aktualumo teisės ir akademiniame kontekste, bet ir dėl asmeninio domėjimosi dirbtiniu intelektu bei jo įtaka žmogaus teisėms. Darbo autorius siekia profesinės karjeros teisės srityje, siejant ją su teisine pagalba dirbtinio intelekto srityje.

Tyrimo problema: Sparčiai vystantis dirbtinio intelekto technologijoms, išryškėja vis daugiau atvejų, kai šios sistemos pažeidžia asmens teisę į privatumą. Nepaisant augančio visuomenės ir teisėkūros dėmesio dirbtinio intelekto technologijai, keliamas klausimas - ar esamas teisinis

[1] „AlexNet and ImageNet: The Birth of Deep Learning“, žiūrėta 2024m. lapkričio 15d. https://www.pinecone.io/learn/series/image-search/imagenet/

reguliavimas yra pakankamas, apsaugoti asmens teisę į privatumą, kai naudojamos dirbtinio intelekto technologijos?

Tyrimo tikslas: Išanalizuoti dirbtinio intelekto technologijų praktikoje keliamas grėsmes asmens teisei į privatumą bei įvertinti šių grėsmių teisinį reguliavimą remiantis analizuotais atvejais.

Tyrimo objektas: Dirbtinio intelekto technologijų taikymo poveikis asmens teisės į privatumą apsaugai.

Tyrimo uždaviniai:

1. Paaiškinti dirbtinio intelekto sampratą, raidą ir pagrindines technologijos savybes.

2. Paaiškinti asmens teisės į privatumą sampratą bei jos apsaugos reikšmę dirbtinio intelekto kontekste.

3. Nustatyti dabartinį asmens teisės į privatumą teisinį reglamentavimą dirbtinio intelekto kontekste.

4. Ištirti dirbtinio intelekto technologijų taikymo praktinį poveikį asmens teisės į privatumą apsaugai, analizuojant „Clearview AI“ ir „Cambridge Analytica“ atvejus.

Ginamieji teiginiai:

1. Dirbtinio intelekto technologija savaime nėra grėsmė asmens teisei į privatumą. Grėsmė kyla atvejais kuomet veiksmus atlieka dirbtinio intelekto sistemų kūrėjai ar naudotojai, priimdami sprendimus, kurie lemia kaip ir kokiais tikslais dirbtinio intelekto technologija bus taikoma.

2. Efektyvi privatumo apsauga priklauso ne tik nuo teisinio reguliavimo, bet ir nuo vartotojų sąmoningumo ir technologijų kūrėjų atsakomybės.

3. Europos Sąjungos Dirbtinio intelekto aktas žymi reikšmingą žingsnį siekiant užtikrinti asmens duomenų apsaugą bei teisę į privatumą, atsižvelgiant į naujausius DI technologijų keliamus iššūkius.

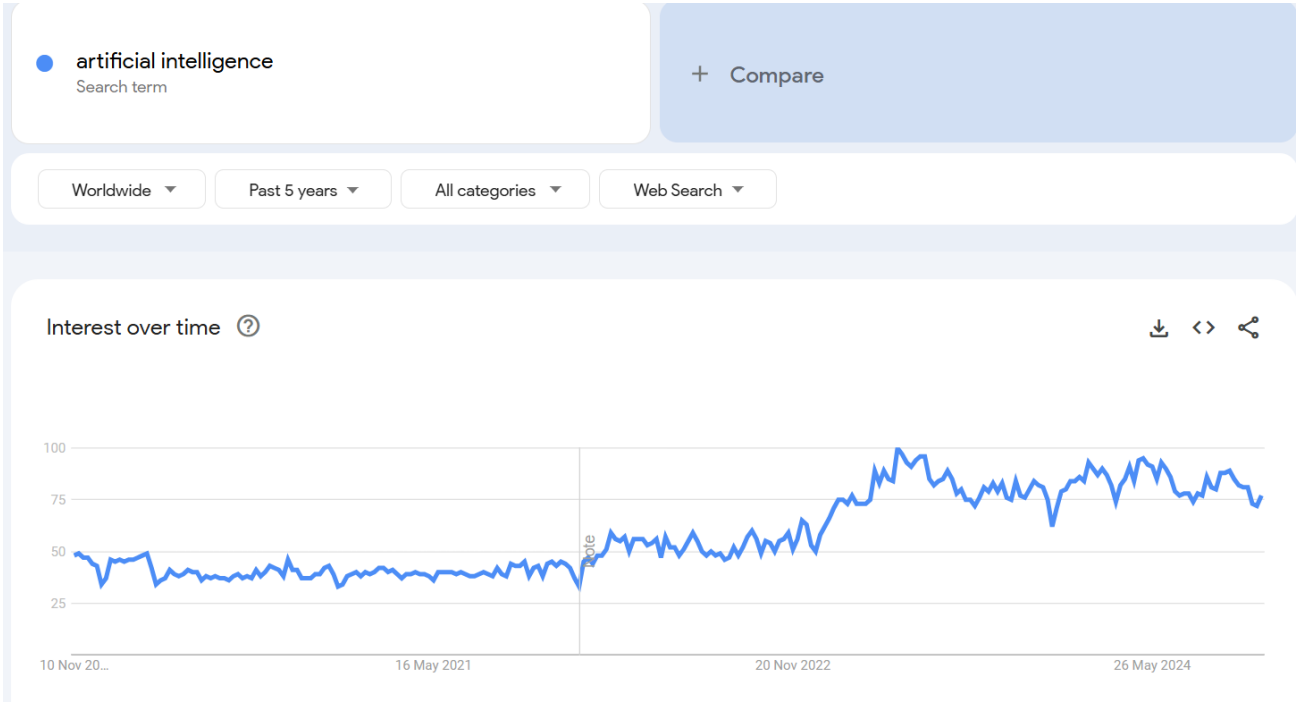
Tyrimo metodologija:

Darbe naudoti teoriniai tyrimo metodai - lyginamasis, kuriuo palyginamas esamas teisinis reguliavimas su naujuoju ES Dirbtinio intelekto aktu. Istorinis, siekiant atskleisti dirbtinio intelekto technologijų vystymosi eigą, suprasti kaip istorinė raida paveikė šiandienines privatumo apsaugos problemas. Tyrime taikytas ir kokybinis tyrimo metodas – atvejo studija. Tyrimo pagrindas – dviejų konkrečių atvejų „Clearview AI“ ir „Cambridge Analytica“ įmonių tyrimas, siekiant suprasti kaip dirbtinio intelekto taikymas gali paveikti asmens teisę į privatumą, taip pat kaip praktikoje pasireiškia grėsmės asmens teisei į privatumą, bei kokiais būdais į tai reaguoja teisėtvarkos objektai.

1. DIRBTINIO INTELEKTO SAMPRATA, RAIDA IR PAGRINDINĖS SAVYBĖS

Naujausiojo amžiaus skirtingų kartų žmonės, nuo brandžiosios iki Y kartų, apie tokius dalykus, kaip kalbėjimas su virtualiais skaitmeniniais asistentais, autonominius automobilius, piešinius, muzikos ir kitus kūrinius, sukurtus kompiuterinės programos, veido, pirštų antspaudų automatinio atpažinimo sistemas, galėjo regėti tik savo fantazijose arba, dalis jų, galėjo tai matyti įvairiuose kino filmuose apie ateitį. Tačiau šiandien, tokie dalykai nėra fantazijos, tai šiuolaikinio žmogaus realybė, vis smarkesniu pagreičiu tampanti ir kasdienybe. Tokią formuojamą kasdienybę lemia gana naujas technologinis reiškinys – dirbtinis intelektas.

Faktą, kad dirbtinio intelekto reiškinys šiandien yra neatsiejamas nuo visuomenės, galima pagrįsti „Google Trends“ platformos duomenimis. Ši „Google“ platforma leidžia analizuoti žmonių atliekamų paieškų tendencijas „Google“ paieškos sistemoje per tam tikrą laikotarpį. Analizuojant paskutinių 5-erių metų duomenis, nuo 2019m., matoma, kad susidomėjimas, pasauliniu mastu, ieškant informacijos, įvedant frazę „artificial intelligence“ (dirbtinis intelektas) į „Google“ paieškos sistemą, nebuvo žemiau 25 indekso. O nuo 2022m. įvyko stiprus pakilimas, ir nuo tada indeksas nemažėja mažiau 50, o per paskutiniuosius metus laikosi tarp 75 ir 100[2].



[2] “Google trends” duomenys, žiūrėta 2024m. lapkričio 15d. https://trends.google.com/trends/explore?date=today%205-y&q=artificial%20intelligenc&hl=en-GB

Tokie duomenys rodo, kad susidomėjimas dirbtiniu intelektu, šiandieninėje visuomenėje, yra ypač didelis. Tai dar kartą pabrėžia šios temos aktualumą ir poreiki ją tyrinėti, bei skirti dėmesį visuomenės švietimui.

Nepaisant to, kad DI yra viena iš sparčiausiai besivystančių technologijų sričių, atkreiptinas dėmesys, kad, šiai dienai, nėra visuotinai priimto apibrėžimo, kuris vienareikšmiškai apibūdintų šį reiškinį. DI sampratą skirtingai aiškina įvairios mokslo disciplinos – nuo kompiuterių mokslo ir kognityvinių mokslų iki teisės ir etikos. Įvairūs aiškinimai, šiame darbe, bus analizuojami šiame skyriuje vėliau, tačiau tam, kad suprasti dirbtinio intelekto sampratos pagrindą, pirmiausia verta išanalizuoti šios sąvokos sudedamąsias dalis – „dirbtinis“ ir „intelektas“. Abu šie žodžiai turi savo skirtingas reikšmes, o jų derinys suteikia visai naują technologinį kontekstą. Dirbtinis – padarytas, netikras, nenatūralus, tai kas yra sukurta žmogaus[3]. Intelektas – žmogaus sugebėjimas mąstyti, protas, protingumas[4]. Taigi, pirmiausia, išanalizavus šias sąvokas atskirai, galima pastebėti, kad apibendrinant DI – tai yra žmogaus sukurtas netikras protas, gebantis mąstyti įvairiose srityse. Šiame skyriuje bus atskleidžiama dirbtinio intelekto istorinė raida, skirtingi dirbtinio intelekto apibrėžimai, dirbtinio intelekto klasifikacijos, sąvokos daugiaprasmiškumas ir DI svarba bei įtaka.

1.1 Dirbtinio intelekto raida

Dirbtinis intelektas, per paskutiniuosius metus, sulaukė ypatingai daug visuomenės dėmesio, tačiau atkreiptinas dėmesys, kad DI istorinėje raidoje pirmuosius konceptus galima pastebėti dar prieš kompiuterių erą. Vienas iš tokių pavyzdžių – graikų mitologijos pasakojimas apie automatoną Talą. Automatonas tai žodis kuriuo, dažniausiai, graikų mitologijoje, apibūdinamas dirbtinis, metalinis „gyvas“ mechanizmas[5]. Šis mitologinis milžinas buvo pagamintas iš bronzos, jo paskirtis buvo apsaugoti Kretos salą nuo bandančių patekti į ją su tikslu pakenkti[6]. Iš istorijos konteksto, šį mechanizmą galima sulyginti su robotu, nors robotų idėja atrodo moderni, tačiau ši istorija parodo, kad graikai jau antikos laikais tyrinėjo koncepcijas rezonuojančias su dirbtiniu intelektu ir šiuolaikinėmis automatizavimo sistemomis. Tai tik vienas iš pirmųjų pavyzdžių, kai žmonės pradėjo

[3] Lietuvių kalbos žodynas, žiūrėta 2024m. lapkričio 15d. https://www.lietuviuzodynas.lt/zodynas/Dirbtinis
[4] Lietuvių kalbos žodynas, žiūrėta 2024m. lapkričio 15d. https://www.lietuviuzodynas.lt/zodynas/Intelektas
[5] Cambridge dictionary, žiųrėta 2024m. lapkričio 15d. https://dictionary.cambridge.org/dictionary/english/automaton
[6] “The story of Talos”, žiūrėta 2024m. lapkričio 15d. https://eurekacourses.org/the-story-of-talos/

mąstyti apie mechanizmus, galinčius savarankiškai atlikti užduotis. Vėlesniais amžiais ši idėja buvo plėtojama įvairiose mokslo ir filosofijos srityse. Kaip vieną iš reikšmingiausių šioje srityje, galima išskirti XVII a. filosofą ir mokslininką Rene Descartes. Savo knygoje „Samprotavimas apie metodą“, penktojoje dalyje, filososas nagrinėjo sąlygas, būtinas tam, kad gyvūnas ar robotas būtų laikomas intelektualia būtybe. Šios idėjos laikomos vienu iš pirmųjų filosofinių dirbtinio intelekto aptarimų istorijoje. XVII a. Europoje, kuomet buvo sukurta daug automatizuotų mašinų ir žmonės žavėjosi jų ypatumais, Rene Descartes bandė įsivaizduoti galimybę sukurti sudėtingus žmogaus formos mechanizmus, kurie galėtų judėti taip pat kaip mes. Tačiau jis teigė, kad tokios mašinos negalėtų turėti žmogaus intelekto. Filosofo manymu, žmogaus protas yra universalus instrumentas, leidžiantis veikti bet kokioje situacijoje. Tuo tarpu mechanizmai gali veikti tik pagal iš anksto numatytą funkciją, kuri buvo sukurta jų kūrėjų[7]. Descartes idėjos ir ankstyvieji mąstymai apie mechanizmų galimybes tapo įkvėpimu vėlesniems moksliniams ir technologiniams bandymams. Nors šie filosofiniai samprotavimai dar buvo toli nuo praktinio dirbtinio intelekto įgyvendinimo, jie padėjo pagrindą diskusijoms apie mąstymo, sąmonės ir mašinų galimybes. Tik XIX a. pabaigoje ir XX a. pradžioje šios idėjos pradėjo virsti realiais technologiniais eksperimentais. DI istorinę raidą galima skaidyti pagal jo vystymosi laikotarpius:

1950–1970 m.: optimizmo era.

1970–1980 m.: dirbtinio intelekto „žiemos“ laikotarpis.

1980–2000 m.: ekspertų sistemų ir mašininio mokymosi pradžia.

2000–dabar: giluminis mokymasis ir praktinės DI taikymo sritys.

Pirmieji žingsniai, kuriais buvo pereita nuo filosofinių apmąstymų prie praktinio dirbtinio intelekto kūrimo, pradėti dėti XX a. viduryje. 1950 m. Alan Turing publikavo savo garsųjį straipsnį „ Computing Machinery and Intelligence“. Šis straipsnis tapo kertiniu akmeniu, žyminčiu dirbtinio intelekto mokslo pradžią. Jis prasideda nuo sakinio „Siūlau apsvarstyti klausimą – ar mašinos gali mąstyti?“[8]. Straipsnyje aptartas mašinų gebėjimas mąstyti ir pasiūlytas garsusis Tiuringo testas, kaip būdas nustatyti, ar mašina gali būti laikoma protinga. Šis testas atliekamas dalyvaujant dviem žmonėms ir kompiuteriui. Testo principas vyksta žaidimu - vienas žmogus, teksto žinutėmis, bendrauja tiek su kitu žmogumi tiek su kompiuteriu, o testas išlaikomas, jeigu žmogus neatskiria su

[7] Masahiro Morioka „Descartes and Artificial Intelligence". *Journal of Philosophy of Life* (2023):1-4, žiūrėta 2024m. lapkričio 16d.
https://www.philosophyoflife.org/jpl2023si_intro.pdf
[8] C. Smith, B. McGuire, T.Huang, G. Yang, „The history of artificial intelligence“, žiūrėta 2024m. lapkričio 16d. https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf

kuo tuo metu bendrauja, ar kitu žmogumi ar kompiuteriu[9]. Alanas Turingas tikėjo, kad po 50 – ies metų kompiuteris gebės taip gerai žaisti tokį žaidimą, kad pasieks 70 procentų laimėjimo rezultatus. Šiandien , praėjus 74 -eriems metams, galima siekti išvadų, kad A. Turingas buvo teisus. Atsižvelgiant į egzistuojančias sistemas, tokias kaip „Google Duplex“, kurios, kaip pavyzdys, naudojant DI pagalba, gali paskambinti į kirpyklą ir bendraujant su kirpėja telefonu užregistruoti žmogų kirpimui[10]. Tačiau praktinis dirbtinio intelekto mokslo vystymas įgavo didesnį pagreitį praėjus keliems metams po jo darbo – įvykus istorinei Dartmouth'o konferencijai 1956 m. Ši konferencija tapo pirmuoju sistemingu mėginimu mokslo pasaulyje oficialiai apibrėžti ir įtvirtinti dirbtinio intelekto mokslą kaip savarankišką tyrimų sritį. Kompiuterių mokslų pradžia, sparčiai didėjantis domėjimasis intelektualiomis mašinomis, įtakojo sąlygas šiai konferencijai įvykti. Konferencijos organizatorių – John McCarthy, Marvin Minsky, Nathaniel Rochester ir Claude Shannon pagrindinis tikslas buvo atlikti dirbtinio intelekto tyrimus ir ištirti galimybes sukurti sistemas, kurios galėtų imituoti žmogaus intelektą, naudojant matematines, logines bei inžinerines metodikas[11]. Konferencijos dalyviai taip pat siekė įtvirtinti DI mokslą kaip atskirą discipliną, atskiriant nuo kitų mokslo sričių bei ištirti kaip mašinos galėtų mokytis, tobulėti ir spręsti įvairias problemas loginiu būdu. Konferencijos rezultatai nebuvo pasiekti kaip praktiniai proveržiai DI mokslo srityje, tačiau ji tapo kertiniu tašku, kuris įtvirtino dirbtinio intelekto mokslo savarankiškumą bei paskatino tolimesnius DI tyrimus. Šio laikotarpio tyrėjai tikėjo, kad DI gebės greitai išspręsti sudėtingas problemas ir atlikti daugelį žmogaus intelektinių užduočių. Dėl šių optimistinių lūkesčių 1950–1970 m. dažnai vadinama optimizmo era, kuri buvo pažymėta svarbiais DI pasiekimais, tokiais kaip 1958 m. sukurtas „LISP“ – pirmoji programavimo kalba, specialiai skirta DI, bei 1966 m. „ELIZA“ – pirmoji pokalbių programa, galinti imituoti žmogaus bendravimą. Ši dirbtinio intelekto era pasižymėjo labai stipriu tikėjimu proveržiu, tačiau dėl didelių lūkesčių, finansavimo sumažėjimo, nepavykus įgyvendinti pernelyg ambicingų tikslų, progresas sustojo ir nuo 1970m. iki 1980m. vyko vadinamasis „žiemos“ laikotarpis dirbtinio intelekto kontekste. Tokį laikotarpį taip pat lėmė nepakankami kompiuterių pajėgumai ir prastas praktinis pritaikymas. Nepaisant DI „žiemos“ laikotarpio, 1980-aisiais pradėjus vystytis ekspertų sistemoms, dirbtinio intelekto tyrimai įgavo naują impulsą. Šis atsigavimas kartu su technologijų

[9] A.M. Turing, „Mind a quarterly review of psychology and philosophy“. *Mind*, (1950): 1–28, žiūrėta 2024m. lapkričio 16d. https://www.eliassi.org/turing-mind-1950.pdf

[10] „Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone“, žiūrėta 2024m lapkričio 16d. https://research.google/blog/google-duplex-an-ai-system-for-accomplishing-real-world-tasks-over-the-phone/

[11] J. McCarthy, M.L Minsky, N. Rochester, C.E. Shannon „A proposal for the Dartmouth summer research project on artificial intelligence“, žiūrėta 2024m. lapkričio 17d. https://raysolomonoff.com/dartmouth/boxa/dart564props.pdf

pažanga ir didėjančiu kompiuterių pajėgumu atvėrė duris naujoms koncepcijoms, kurios pasiekė pirmąjį proveržį 1990-aisiais – mašininio mokymosi pradžia[12]. Mašininis mokymasis tapo kertiniu žingsniu, leidusiu DI sėkmingai išspręsti specifines problemas ir toliau vystytis iki šių dienų. Mašininis mokymasis yra specializuotas dirbtinio intelekto pogrupis, kuriame algoritmai kuriami remiantis duomenimis, o ne iš anksto užprogramuotomis taisyklėmis. Šiame procese žmogus padeda algoritmams, parinkdamas svarbiausias duomenų savybes, kurios reikalingos konkrečiai užduočiai spręsti. Pavyzdžiui, norint, kad algoritmas atpažintų šunį nuotraukoje, žmogus nurodo kokias savybes algoritmas turėtų atpažinti – keturias kojas, uodegą, ausis, snukio formą ir pan.. Tada algoritmas mokomas atskirti šunį nuo kitų objektų, remiantis šiais apibrėžtais kriterijais. Po mašininio mokymosi sėkmės, 1990-aisiais, dirbtinio intelekto tyrimai su laiku dar labiau intensyvėjo ir giluminio mokymosi srityje. Giluminis mokymasis, pasitelkęs dirbtinius neuroninius tinklus, tapo pagrindiniu įrankiu sprendžiant sudėtingas problemas, tokias kaip kalbos atpažinimas, vaizdų analizė ir tekstų generavimas, tai mašininio mokymosi metodas, kuris leidžia kompiuteriams mokytis iš didelių duomenų rinkinių automatiškai, be žmogaus tiesioginio įsikišimo. Šis metodas naudoja daugiasluoksnius neuroninius tinklus, kurie analizuoja duomenis, žingsnis po žingsnio, pradedant nuo paprastesnių savybių, tokių kaip linijos, spalvos pereinant į sudėtingesnes struktūras, tokias kaip šunio formos ar atpažįstami bruožai.[13]. Mašininio ir giluminio mokymosi skirtumus galima paaiškinti pasitelkiant paprastą pavyzdį, įsivaizduojant, kad yra vaikas, kurį reikia išmokyti kaip atrodo šuo. Mašininio mokymosi principu vaikui padedama mokytis, nurodant ko ieškoti, pvz. – šunys turi keturias kojas ir uodegą, o giluminio mokymosi principu, vaikas pats mokosi, analizuodamas tūkstančius šunų nuotraukų, ir tokiu būdų jis atranda kaip šunys atrodo be išankstinio mokytojo paaiškinimo.

Nors dirbtinio intelekto technologijos ilgus metus vystėsi lėtai, dėl ribotų resursų ar teorinių ribų, šiandieninėje visuomenėje DI tapo vienu iš svarbiausių mokslo ir technologijų pažangos įrankiu. Giluminio mokymosi algoritmai, taikomi įvairioms sudėtingoms užduotims atlikti, kuria vis naujesnes ir stipresnes galimybes panaudoti DI tokiose srityse kaip medicininė diagnostika, transportas, švietimas ir palengvinti begalę kitų žmogaus kasdienių veiklų įvairiose srityse. Tačiau, atkreiptinas dėmesys, kad šiuo metu esanti greita DI raida kelia ir naujų iššūkių, pradedant nuo etinių dilemų iki grėsmių asmens privatumui. Norint suprasti kaip siekti šios technologijos reguliavimo ir kontrolės,

[12] „What is the history of artificial intelligence?“ Tableau, žiūrėta 2024m. lapkričio 17d., https://www.tableau.com/data-insights/ai/history

[13] Y. Lecun, Y. Bengio, G. Hinton “Deep learning”. *Nature,* (2015): 436-444 , žiūrėta 2024m. lapkričio 17d. https://hal.science/hal-04206682/document

būtina detaliau išanalizuoti DI sampratą ir jos skirtingus apibrėžimus, detalesnė analizė taip pat padės atskleisti šio reiškinio daugiaprasmiškumą.

1.2 Dirbtinio intelekto samprata

Analizuojant dirbtinio intelekto sampratą svarbu dar kartą akcentuoti, kad šiandien nėra vieningo apibrėžimo ar nuomonės, kurios būtų taikomos visuotinai apibrėžiant DI sąvoką. Tokią dabartinę situaciją nulėmė šios technologijos naujumas. Apibrėžimai gali skirtis priklausomai nuo mokslo disciplinos ar taikymo srities. Skirtingų apibrėžimų analizė leidžia ne tik suprasti kaip šis reiškinys suvokiamas įvairiuose kontekstuose, bet ir atskleisti kokie aspektai yra akcentuojami DI tyrimuose bei praktikoje. Akademiniame kontekste DI apibrėžimas taip pat aiškinamas įvairiai, todėl šiame darbe bus aptariamos keleto skirtingų mokslininkų nuomonės, kurios turi tarptautinį pripažinimą.

1956 metais dirbtinio intelekto terminą pirmą kartą pavartojo amerikiečių kompiuterių mokslininkas John McCarty, Dartmuto konferencijoje jis pasiūlė tokį apibrėžimą – „Dirbtinis intelektas yra mokslas ir inžinerija, skirti kurti protingas mašinas.“[14] Šiame mokslininko pasiūlytame apibrėžime atsiskleidžia dvi pagrindinės DI srities kryptys. Mokslinė pusė – tai tyrimai ir teorijų kūrimas apie tai kaip mašinos galėtų imituoti intelektą, bei inžinerinė pusė – praktinis sistemų su intelektu kūrimas. Nors apibrėžimas atrodo ganėtinai paprastas, jis tapo pagrindu daugeliui vėlesnių apibrėžimų.

Sekant J. McCarthy apibrėžimu, kuris pabrėžia mokslinius ir inžinerinius DI aspektus, kito amerikiečių kompiuterių mokslininko Nilso Johno Nilssono apibrėžimas nukreipia dėmesį į praktinį pritaikymą. Savo knygoje „The Quest for Artificial Intelligence“ jis pateikė apibrėžimą – „dirbtinis intelektas yra veikla, skirta sukurti mašinas, kurios būtų protingos. O intelektas yra ta savybė, kuri leidžia subjektui tinkamai veikti ir numatyti ateities įvykius savo aplinkoje[15].” Paprasčiau tariant, šio mokslininko apibrėžimas reiškia tokių sistemų kūrimą , kurios galėtų pakeisti žmogų užduotyse, kur paprastai reikalingas žmogaus intelektas. Šis apibrėžimas svarbus keliais aspektais, jame akcentuojamas praktinis pritaikymas, ne tik teoriniai aspektai, išskiriamas tikslas sujungti technologijas ir žmogaus gebėjimus.

[14] John McCarthy, „What is artificial intelligence?“. Formal Stanford , žiūrėta 2024m. lapkričio 28d. https://www-formal.stanford.edu/jmc/whatisai.pdf

[15] Nils J. Nilsson „The quest for artificial intelligence a history of ideas and achievements". Stanford, žiūrėta 2024m. lapkričio 28d. https://ai.stanford.edu/~nilsson/QAI/qai.pdf

Dar vienas reikšmingas dirbtinio intelekto apibrėžimas yra pateiktas Stuart Russell ir Peter Norvig darbe. Jų požiūris pabrėžia, kad DI esmė – gebėjimas sąveikauti su aplinka ir priimti sprendimus, orientuotus į konkrečių tikslų pasiekimą. Pasak šių autorių, DI sistemos turėtų ne tik mokytis ar imituoti žmogaus intelektą, bet ir efektyviai prisitaikyti prie kintančių aplinkybių.[16] Toks apibrėžimas svarbus keliais aspektais. Pirmiausia šis apibrėžimas orientuotas į praktinius DI taikymo aspektus, tai yra į sprendimų priėmimą ir tikslų siekimą. Taip pat šis apibrėžimas pabrėžia ir sistemos gebėjimą pačiai efektyviai veikti įvairiose situacijose. S. Russell ir P. Norvig apibrėžimas išlieka aktualus ir šiuolaikiniam DI taikymui. Tokiose srityse kaip autonominių transporto priemonių sistemos, prognozavimo modeliams ar virtualiems asistentams kaip „Alexa“ ir „Siri“. Mokslininkų pateikti apibrėžimai pabrėžia tiek teorinius, tiek praktinius DI aspektus – nuo intelekto imitacijos ir mokymosi iki gebėjimo prisitaikyti prie kintančių aplinkybių. Akademiniai apibrėžimai ne tik formuoja teorinį DI pagrindą, bet ir padeda struktūruoti tolimesnius šios technologijos tyrimus bei plėtrą.

Vis dėlto, be akademinio požiūrio, dirbtinis intelektas yra intensyviai nagrinėjamas ir technologijų kūrėjų bei taikytojų. Technologinis požiūris atskleidžia kaip DI yra suvokiamas praktikoje – tiek kuriant, tiek diegiant sprendimus įvairiose srityse. Šis požiūris suteikia galimybę pažvelgti į DI kaip įrankį, kuris ne tik sprendžia sudėtingas problemas, bet ir keičia kasdieninį gyvenimą, verslą bei pramonę. Technologijų kūrėjų ir pramonės atstovų požiūriu dirbtinis intelektas yra esminis įrankis, leidžiantis automatizuoti procesus, didinti efektyvumą ir kurti naujoviškus sprendimus įvairiose srityse. Pavyzdžiui, „Google“ naudoja DI savo paieškos algoritmų tobulinimui, siekdama pateikti tikslesnius ir labiau tinkamus rezultatus vartotojams[17]. „Amazon“ taiko DI personalizuotoms produktų rekomendacijoms generuoti, analizuodama vartotojų elgseną ir pirkimo istoriją[18]. Tuo tarpu „Tesla“ diegia DI technologijas autonominių transporto priemonių valdymui, siekdama sukurti visiškai savarankiškai veikiančius automobilius. DI integruojamas į įvairias pramonės šakas tokias kaip gamyba, logistika, finansai ir medicina. Pavyzdžiui, medicinoje DI naudojamas diagnostinių vaizdų analizei, padedant aptikti ligų požymius ir pasiūlyti tinkamus

[16] S. Russel, „P. Norvig Artificial intelligence a modern approach". Upper Saddle River, New Jersey: Pearson education, 1955. žiūrėta 2024m. lapkričio 28d.
https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf
[17] „Google Ai principles“.Google, žiūrėta 2024m. lapkričio 28d.
https://ai.google/static/documents/EN-AI-Principles.pdf
[18] „How Amazon is using generative AI to improve product recommendations and descriptions“. About Amazon, žiūrėta 2024m. lapkričio 28d.
https://www.aboutamazon.com/news/retail/amazon-generative-ai-product-search-results-and-descriptions

gydymo būdus[19]. Tokie taikymai ne tik padidina procesų efektyvumą, bet ir sumažina klaidų tikimybę taip gerinant paslaugų kokybę ir patikimumą.

Technologinis požiūris į DI pabrėžia jo praktinę naudą ir gebėjimą spręsti realias problemas, todėl DI tampa neatsiejama šiuolaikinių technologijų ir inovacijų dalimi. Nors skirtingi požiūriai padeda suprasti dirbtinio intelekto sąvokos įvairovę bei jos taikymo galimybes, tačiau to nepakanka norint išsamiai ir detaliai įsigilinti į dirbtinio intelekto sampratą.

1.3 Dirbtinio intelekto klasifikacija

Dirbtinio intelekto sampratos analizė būtų neišsami neaptarus jo klasifikacijos. Dirbtinio intelekto klasifikavimas leidžia ne tik išskirti jo skirtingas savybes ir veikimo principus, bet ir geriau suprasti jo taikymo ribas bei galimybes. Kaip pagrindines dirbtinio intelekto klasifikavimo kryptis galima išskirti į tris rūšis. Pagal intelekto lygį, pagal veikimo principą ir pagal taikymo sritį.

Pagal intelekto lygį išskiriamos šios rūšys:

1. Silpnas DI (anglų k. Narrow AI) – šio dirbtinio intelekto tipas naudojamas atlikti vienai konkrečiai užduočiai atlikti. Silpnas DI neturi galimybės mąstyti, tokia mašina atlieka iš anksto nustatytas funkcijas. Taip veikia įvairios telefonų programos, atpažinimo įrankiai, šlamšto filtrai ir kt. Pavyzdžiui „Siri“ ar „Google vertėjas“.

2. Stiprus DI (anglų k. General AI) – dar vadinamas bendruoju dirbtiniu intelektu, šiandien kol kas išlieka tik teoriniu konceptu. Stiprusis DI turėtų gebėti atlikti bet kokią užduotį, kurią gali atlikti žmogus, panaudojant savo intelektą, kūrybinį mąstymą, socialinį supratimą ir gebėjimą mokytis bei prisitaikyti prie nematytų situacijų be išankstinio programavimo.[20]

Pagal veikimo principą[21]:

1. Reaktyviosios mašinos – tokios mašinos veikia tik pagal turimus duomenis. Jos neturi gebėjimo atsiminti praeitų savo įvykių priimant naujus sprendimus. Vienas iš garsiausių tokios

[19] Christoper Mims, „A Powerful AI Breakthrough Is About to Transform the World“. The Wall Street Journal, žiūrėta 2024m. lapkričio 28d.
https://www.wsj.com/tech/ai/a-powerful-ai-breakthrough-is-about-to-transform-the-world-095b81ea?
[20] Naveen Joshi, „7 Types of artificial intelligence". Forbes, žiūrėta 2024m., gruodžio 2d.
https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificial-intelligence/?sh=45e12add233e
[21] Omar Santos, Petar Radanliev „Beyond the Algorithm: AI, Security, Privacy, and Ethics". Pearson Education: 2024 ,žiūrėta 2024m. gruodžio 2d.
https://www.google.lt/books/edition/Beyond_the_Algorithm/QHriEAAAQBAJ?hl=lt&gbpv=0

mašinos pavyzdžių, 1990 – ais metais įveikęs Garį Kasparovą, šachmatų kompiuteris „IBM Deep Blue“[22]

2. Ribotos atminties – šis tipas geba atlikti sudėtingas klasifikavimo užduotis, prisiminti duomenis ir atlikti prognozes. Tokiu principu veikia savaeigiai automobiliai, tačiau susidūrus su neįprasta užduotimi mašina nesusitvarkys, pavyzdžiui pamačius naują kelio ženklą kurio nėra atmintyje. Tai yra dabartinė dirbtinio intelekto būklė.

3. Proto ir savivokos teorijos – šiuo metu siekiama sukurti sistemas, galinčias suprasti kitų žmonių ar objektų mintis, emocijas ir ketinimus. Veikiant tokiai technologijai, ji sugebėtų priimti sprendimus atsižvelgiant į žmogaus įsitikinimus ir emocijas. Savivokos teorija – tai teorinis DI tipas, aukščiausias raidos lygis, kuomet mašina galėtų atpažinti save ir pati analizuoti savo veiksmus.

Pagal taikymo sritį[23]:

1. Gamtinės kalbos apdorojimas (NLP) – geba suprasti, analizuoti ir generuoti natūralią žmogaus kalbą, pavyzdžiui ChatGPT kalbos modelis.

2. Kompiuterinė rega – atlieka vaizdų analizę ir atpažinimą, pavyzdžiui veido atpažinimo sistemos.

3. Ekspertų sistemos – programos sprendžia specifines problemas, naudojant taisyklių bazę ir turimas žinias, pavyzdžiui medicinos diagnostikos sistemos.

4. Robotika – tai dirbtinio intelekto naudojimas mechaninių sistemų valdymui ir automatizacijai, pavyzdžiui pramoniai robotai, autonominiai dronai.

DI samprata, jo raida ir klasifikacijos atskleidžia sudėtingą ir daugiaprasmį šios technologijos pobūdį. Jo ištakos siekia nuo mitologinių pasakojimų, filosofinių apmąstymų, o per dešimtmečius ši technologija tapo aktualiausia mokslo ir technologijų sritis. Istorinės raidos kontekste, pradedant nuo A. Turingo iki Darmouth‘o konferencijos, DI atsiskleidė kaip pažangi inovacija, kuri turi didelį poveikį įvairioms gyvenimo sritims. Analizuojant skirtingus apibrėžimus, atsiskleidžia dirbtinio intelekto suvokimo dinamiškumas ir priklausomybė nuo požiūrio – akademinio, technologinio ar praktinio. Mokslininkai, tokie kaip John McCarthy, Nils John Nilsson kartu su Stuart Russel bei Peter Norvig, pabrėžė tiek intelektinės imitacijos, tiek sprendimų priėmimo svarbą, o technologijų kūrėjai ir pramonės atstovai dirbtini intelektą laiko įrankiu, kuris tampa neatsiejamu norint efektyvumo ir inovacinių pasiekimų.

[22] IBM History „Deep blue“. IBM, žiūrėta 2025m. gruodžio 2d. https://www.ibm.com/history/deep-blue
[23] „The Applications of AI in Natural Language Processing, Computer Vision, and Speech Recognitio", žiūrėta 2024m. gruodžio 2d. https://futureskillsprime.in/knowledge-center/tech-simplified/applications-ai-natural-language-processing-computer-vision-and-speech-recognition

DI klasifikacija dar labiau išplečia šią sampratą, atskleidžiant intelekto lygius, veikimo principus ir taikymo sritis. Silpnojo ir stipriojo DI skirtumai padeda suvokti, kokius tikslus šiuolaikinis DI geba pasiekti šiandien ir kokios užduotys gali būti įveikiamos netolimoje ateityje. Taikymo sritys parodo kaip DI įsitvirtina kasdieninėje veikloje. Įprastai, lengvai prieinamuose šaltiniuose, dirbtinis intelektas apibrėžiamas kaip programine įranga grindžiamos virtualiosios technologijos, kurios demonstruoja protingą ir sumanų elgesį. Tačiau toks apibrėžimas yra paviršutiniškas ir to neužtenka norint pilnai suprasti DI ir analizuoti jo keliamas grėsmes. Todėl išsamesnis sampratos atskleidimas yra vienas iš esminių žingsnių siekiant suprasti kokį poveikį šis reiškinys daro šiuolaikinėje visuomenėje. Nors šiame skyriuje gana plačiai aptarta dirbtinio intelekto samprata, istorija, apibrėžimai, klasifikacijos, atkreiptinas dėmesys, kad DI taikymo sritys yra svarbios grėsmių į privatumą kontekste, todėl vėliau šiame darbe, remiantis taikymo sritimis, bus siekiama atskleisti realias grėsmės privatumui, kurias gali sukelti tokios sritys kaip veido atpažinimo sistemos, kalbos modeliai ar kitos, keliančios riziką, sritys. Tačiau prieš tai svarbu suprasti asmens teisės į privatumą, grėsmės sampratas, bei teisinį reglamentavimą, kas bus aptarta kitoje darbo dalyje.

2. ASMENS TEISĖS Į PRIVATUMĄ SAMPRATA

Norint suprasti asmens teisės į privatumą esmę, pirmiausia verta apžvelgti sąvokų „privatus“ ir „privatumas“ reikšmes. Lietuvių kalbos žodyne, terminas „privatus“ reiškia asmeninį, nesusijusį su valstybės institucijomis ar viešaisiais reikalais, o „privatumas“ kaip šio termino išvestinė sąvoka, nurodo atskirumą, slaptumą, konfidencialumą. Ši sąvoka pabrėžia individo laisvę pasirinkti ką jis nori atskleisti kitiems ir kokią informaciją pasilaikyti sau[24]. Tai išryškina esminį privatumo elementą – informacinį savarankiškumą, kuris tampa vis aktualesnis skaitmeniniame amžiuje.

Privatumo samprata nesusiformavo per naktį. Teigiama, kad diskusijos apie privatumo klausimus yra tokios senos, kaip ir pati žmonija[25]. Filosofijos istorijoje Aristotelis yra laikomas vienu pirmųjų mąstytojų, kuris išskyrė privačią sferą iš viešosios[26]. Savo politinės filosofijos darbuose jis apibrėžė dvi pagrindines žmonių gyvenimo sritis – *oikos* (privačią sferą) ir *polis* (viešąją sferą). *Oikos*

[24] Lietuvių kalbos žodynas, žiūrėta 2024m. gruodžio 2d.
[25] J. Holvast, „History of Privacy“. The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology, vol 298. Springer, Berlin, Heidelberg, žiūrėta 2024m. gruodžio 2d.
https://link.springer.com/chapter/10.1007/978-3-642-03315-5_2
[26] DeCew, Judith „Privacy“. *Stanford encyclopedia of philosophy arhcive* (2018), žiūrėta 2024m. gruodžio 2d.
https://plato.stanford.edu/archives/spr2018/entries/privacy/

apėmė šeimos ir namų gyvenimą, susijusį su asmenine ekonomine veikla, emociniais ryšiais ir vidiniais reikalais, kuriuose viešosios politikos ar visuomenės interesai neturėjo kištis. Tuo tarpu *polis* buvo viešoji erdvė, kurioje vyko politinės diskusijos, buvo priimami įstatymai ir užtikrinama bendruomenės gerovė. Šis viešosios ir privačiosios sferų atskyrimas padėjo pamatą pirminei privatumo sampratai, pabrėžiant, kad tam tikros gyvenimo sritys turi būti apsaugotos nuo viešo kišimosi. Aristotelio mintys įkvėpė vėlesnes filosofines ir teisines doktrinas, kuriomis buvo siekiama apibrėžti individo ir valstybės santykio ribas.

Romėnų teisė vėliau praplėtė šią sampratą, bandydama teisiškai apginti asmens privatumą. Romos laikais buvo įtvirtintas principas *domus sua cuique est tutissimum refugium*, reiškiantis - „Kiekvieno namai yra saugiausias prieglobstis“. Nors tiksli šio posakio kilmė nėra aiškiai nustatyta, kai kurie šaltiniai teigia, kad jis priskiriamas romėnų valstybės veikėjui ir oratoriui Ciceronui[27]. Tačiau kiti šaltiniai nurodo, kad šis posakis buvo įtvirtintas anglų teisininko sero Edvardo Koko. 1628 m. veikale „The Institutes of the Laws of England“[28]. Nepaisant to, posakis atspindi seną teisės principą, kuris pabrėžian namų neliečiamumą ir asmens teisę į saugumą savo gyvenamojoje vietoje. Romėnų teisės tradicijos, kartu su graikų ir anglosaksų teisės kodeksais, padėjo pagrindus šiuolaikinei privatumo teisei. Toks požiūris suformavo vienus iš pirmų žmogaus teisių kontūrų, kuriuose privati erdvė laikoma neliečiama vertybe.

Nepaisant to, kad pradinė privatumo samprata buvo orientuota į fizinės erdvės ir kūno neliečiamumo apsaugą, ilgainiui šis suvokimas išsiplėtė ir apėmė asmens informacijos kontrolę. Modernesnis privatumo, kaip teisinio reiškinio, suvokimas atsirado XIX a. pabaigoje. 1890 m. amerikiečių teisininkai Samuel D. Warren ir Louis D. Brandeis paskelbė revoliucinį straipsnį „Teisė į privatumą“ (*The Right to Privacy*). Šiame darbe autoriai privatumą apibūdino kaip „teisę būti paliktam vienam“. Jie pabrėžė, kad technologinė pažanga, tokia kaip momentinė fotografija ir laikraščių plėtra, kelia naujų grėsmių asmens privatumui[29]. Šis straipsnis tapo vienu kertinių akmenų moderniai privatumo sampratai, kuri pradėta laikyti neatsiejama žmogaus teise. Ši publikacija įtvirtino nuostatą, kad teisė į privatumą nėra tik fizinės apsaugos klausimas, bet ir informacijos srauto valdymo galimybė.

---

[27] „Domus sua cuique est tutissimum refugium“ RunSensible’s Legal Dictionary, žiūrėta 2024m. gruodžio 3d. https://www.runsensible.com/legal-dictionary/domus-sua-cuique-est-tutissimum-refugium/

[28] „Oxford Essential Quotations“. Oxfard Reference, žiūrėta 2024m. gruodžio 3d. https://www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00003117?

[29] Samuel D. Warren, Louis D. Brandeis, „The right to privacy". *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), pp. 193-220. žiūrėta 2024m. gruodžio 3d. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

Teisės į privatumą samprata toliau vystėsi Jungtinėse Amerikos Valstijose, kur šia tema aktyviai domėjosi ir ją gilino įvairūs teisės teoretikai. Pavyzdžiui, W. Prosser laikė, kad ši teisė apima apsaugą nuo klaidinančios ar trikdančios informacijos apie asmenį paskleidimo[30]. Tuo tarpu A. F. Westin pabrėžė asmens galimybę pačiam kontroliuoti kokia informacija apie jį, kokiu būdu ir kokiu metu gali būti atskleista kitiems.[31] W. A. Parent akcentavo, kad privatumas – tai būsena, kai kiti neturi prieigos prie duomenų apie asmenį, nebent tokie duomenys jau yra viešuose šaltiniuose.[32] Savo ruožtu J. De Cew siūlė platesnį požiūrį – pasak jo, privatumas apima tiek informacijos kontrolę, tiek asmens fizinio ir psichinio neliečiamumo užtikrinimą, kartu ir laisvę priimti svarbius gyvenimo sprendimus, susijusius su šeima ar asmeniniu gyvenimo būdu.[33]

Aristotelio filosofija, romėnų teisinės tradicijos ir XIX a. pabaigos intelektinės diskusijos rodo, kad privatumo samprata ilgainiui plėtėsi ir įgavo vis daugiau aspektų. Nuo fizinės erdvės apsaugos iki teisės kontroliuoti asmeninę informaciją, privatumas tapo viena iš esminių žmogaus teisių ir neatsiejama modernios visuomenės dalimi. Tokia evoliucija rodo, kad teisė į privatumą formuojasi nuolat, reaguojant ir prisitaikant į naujus visuomenės ir technologijų iššūkius.

Teisė į privatumą tradiciškai buvo suprantama kaip individo teisė į neliečiamą asmeninę erdvę, savarankiškumą ir apsaugą nuo išorinio kišimosi. Šis principas išsivystė nuo fizinės erdvės saugojimo iki teisės kontroliuoti informaciją apie save. Šiuolaikinė visuomenė, nuolat veikiama technologijų progreso, išplėtė šios teisės suvokimą, ypač skaitmeninės erdvės kontekste. DI iš esmės keičia privatumo suvokimą, nes jis geba rinkti, analizuoti ir sisteminti milžiniškus duomenų kiekius. Skaitmeniniai asistentai, biometrinių duomenų atpažinimo sistemos ir elgsenos prognozavimo algoritmai transformuoja privatumą iš fizinės erdvės apsaugos į skaitmeninio savarankiškumo užtikrinimą. Tai reikalauja naujų teisinių, etinių ir technologinių priemonių, kurios galėtų apsaugoti individą šiame dinamiškame technologijų amžiuje. Asmens teisė į privatumą šiandien apima ne tik apsaugą nuo fizinio kišimosi, bet ir gebėjimą kontroliuoti, kaip jo duomenys naudojami skaitmeninėje erdvėje. Dirbtinio intelekto įtaka šiame kontekste yra ypač svarbi, nes ši technologija gali ne tik automatizuoti procesus, bet ir įžvelgti asmenų elgsenos modelius, numatyti jų veiksmus ar net daryti sprendimus, remdamasi surinktais duomenimis.

---

[30] Prosser, William L. „Privacy“. *California law review* (1960) 383, žiūrėta 2024m. gruodžio 4d. https://lawcat.berkeley.edu/record/1109651?v=pdf

[31] A. F. Westin „Privacy and freedom“. *Washington and Lee Law Review* (1968) 1-6 , žiūrėta 2024m. gruodžio 4d. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

[32] W.A. Parent „A new definition of privacy for the law“. *Law and Philosophy*, (1983), 305-338 , žiūrėta 2024m. gruodžio 4d. https://peeps.unet.brandeis.edu/~teuber/Parent_on_Privacy.pdf

[33] J. De Cew „In pursuit of privacy“ , žiūrėta 2024m. gruodžio 4d.

Visa tai iškelia klausimus apie duomenų rinkimo ir naudojimo skaidrumą bei žmogaus teisę į informacijos kontrolę. Atsižvelgiant į šiuos iššūkius, svarbu suprasti kaip teisė į privatumą adaptuojasi dirbtinio intelekto eroje, ypatingą dėmesį skiriant tam, kaip skaitmeninis privatumas keičia tradicinį supratimą. Atkreiptinas dėmesys, kad gilinantis į teisės į privatumo sampratą DI kontekste, atrandamas labai svarbus „raktažodis“ – duomenys. Dirbtinio intelekto kontekste asmens duomenys yra esminė technologijos veikimo dalis – be jų DI negalėtų mokytis, analizuoti ar priimti sprendimų. Duomenų svarba šiuolaikiniame pasaulyje neabejotinai yra viena iš esminių priežasčių, kodėl teisė į privatumą transformavosi ir išsiplėtė. Skaitmeninės technologijos įgalino milžinišką duomenų srautą, kuris apima ne tik pagrindinę informaciją, bet ir išsamius asmeninius profilius, elgsenos modelius, biometrinius rodiklius, geografinės lokacijos duomenis ir dar daugiau. Šiandien duomenys tampa neatsiejama teisės į privatumą dalimi, nes jų rinkimas, kaupimas ir naudojimas tiesiogiai susijęs su asmens autonomija ir jo gebėjimu kontroliuoti informaciją apie save. Asmens duomenų apsauga išplečia teisės į privatumą sampratą, nes šiandien asmens privatumo užtikrinimą apima ne tik fizinės erdvės, bet ir skaitmeninių duomenų neliečiamumas. Tai kelia svarbius klausimus ne tik apie teisę į privatumą, bet ir apie tai, kaip šie duomenys yra apsaugoti nuo piktnaudžiavimo.

Prieš pateikiant teisės į privatumą ir duomenų apsaugos teisinio reglamentavimo analizę, svarbu suvokti ne tik teisės į privatumą reikšmę, bet ir kas yra laikoma asmens duomenimis. Europos Sąjungos Bendrasis duomenų apsaugos reglamentas (GDPR) pateikia gana platų apibrėžimą – „*asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius*[34]“

Kad būtų galima geriau suvokti asmens duomenų apsaugos svarbą teisės į privatumą kontekste, būtina detaliau išanalizuoti, kas tiksliai yra laikoma asmens duomenimis.

a) Tiesioginiai identifikatoriai: vardas ir pavardė, asmens kodas, gimimo data, adresas.

b) Kontaktiniai duomenys: telefono numeris, elektroninio pašto adresas.

c) Demografiniai duomenys: pilietybė, lytis, socialinis statusas

[34] „Bendrasis duomenų apsaugos reglamentas“, žiūrėta 2024m. gruodžio 3d. https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679

d) Biometriniai duomenys: veido atvaizdas. pvz., nuotrauka ar vaizdo įrašas, pirštų atspaudai, akių rainelės vaizdas, balso atpažinimo duomenys.

e) Elektroniniai identifikatoriai: IP adresas, slapukų generuojami identifikatoriai, geografinės lokacijos duomenys, prisijungimo prie tinklo ar sistemos žurnalai.

f) Finansiniai duomenys: banko sąskaitos numeris, kredito kortelės informacija, mokėjimų istorija,

g) Jautrūs asmens duomenys: sveikatos būklė ir medicininė informacija, politinės pažiūros, religiniai ar filosofiniai įsitikinimai, narystė profesinėse sąjungose, rasė ar etninė kilmė, genetiniai duomenys.

e) Profesiniai duomenys: darbo vieta, pareigos, darbo našumo įvertinimai.

Asmens teisė į privatumą su laiku keitėsi, prisitaikydama prie visuomenės pokyčių ir progreso iš technologijų srities. Iš pradžių orientuota į fizinės erdvės neliečiamumą, ši teisė apima vis sudėtingesnius aspektus, tokius kaip duomenų apsauga skaitmeninėje erdvėje. Informacinės technologijos, ypač dirbtinis intelektas, iš esmės keičia privatumo suvokimą, paverčiant asmens duomenis aktualiausia šiandieninėje visuomenėje teisės į privatumą dalimi. Kaip ir kokiu mastu duomenys yra naudojami, kontrolė tampa vienas svarbiausių iššūkių šiuolaikiniame pasaulyje. Todėl toliau šiame darbe bus nagrinėjama, kaip teisės normos reaguoja į šiuos pokyčius ir kokios priemonės užtikrina asmens duomenų ir privatumo apsaugą dirbtinio intelekto eroje.

Apibendrinant, asmens teisė į privatumą – tai gilias šaknis istoriniame, filosofiniame kontekste turinti žmogaus teisė, kuri reaguodama į visuomenės ir technologijų raidą kinta. Nuo privačios fizinės erdvės neliečiamumo iki skaitmeninio duomenų valdymo šiuolaikiniame pasaulyje privatumo samprata išsiplėtė ir tapo visapusiška. Dirbtinio intelekto gebėjimai rinkti, analizuoti asmens duomenis kelia naujus iššūkius, todėl šiandien skaitmeninis žmogaus neliečiamumas tampa ne mažiau svarbus nei fizinis.

3. TEISĖS Į PRIVATUMĄ DIRBTINIO INTELEKTO KONTEKSTE TEISINIS REGLAMENTAVIMAS

Norint suprasti, kaip teisė į privatumą yra apsaugota šiuolaikinėje visuomenėje, būtina analizuoti teisės aktus ir reglamentus, reguliuojančius šią sritį. Teisinis reglamentavimas yra pagrindinis instrumentas, užtikrinantis, kad technologijų pažanga, ypač dirbtinio intelekto plėtra, neprasilenktų su pagrindinėmis žmogaus teisėmis. Bus analizuojami tiek Europos Sąjungos teisės

aktai, tiek Lietuvos nacionaliniai teisės aktai, siekiant įvertinti jų tinkamumą ir veiksmingumą sprendžiant šiuolaikinius privatumo apsaugos iššūkius.

3.1 Europos sąjungos instrumentai

Europa yra laikoma viena iš pagrindinių regionų, kur susiformavo seniausi, išsamiausi ir plačiausiai taikomi duomenų apsaugos reglamentai, užtikrinantys asmens duomenų apsaugą tiek nacionaliniu, tiek regioniniu lygiu. Per savo tarptautines institucijas Europos Sąjunga tapo kertiniu akmeniu, padedančiu formuoti pasaulinę duomenų apsaugos sistemą. ES duomenų apsaugos teisės pagrindų raida išsiskiria keturiais pagrindiniais etapais: (1) nacionalinių duomenų apsaugos režimų kūrimas (1970–1980 m.); (2) tarptautinės apsaugos principų įtvirtinimas (1980–1981 m.); (3) nacionalinis įstatymų įgyvendinimas (1982–1994 m.); ir (4) Europos duomenų apsaugos harmonizavimas (1995–2016/2018 m.).[35]

1950 m. priimta Europos žmogaus teisių ir pagrindinių laisvių konvencija yra pirmasis ir svarbiausias dokumentas, susijęs su Europos Tarybos duomenų apsaugos iniciatyvomis. Konvencija buvo priimta 1950 m. ir įsigaliojo 1953 m. Narystės Europos Taryboje sąlyga buvo šios konvencijos ratifikacija[36]. Tarp daugelio kitų dalykų, Konvencija saugo teisę į asmeninį ir šeimos gyvenimą. Pavyzdžiui, jos 8 straipsnis skelbia: " 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 kelią viešos tvarkos pažeidimams ar nusikaltimams, taip pat žmonių sveikatai ar moralei arba kitų asmenų teisėms ir laisvėms apsaugoti.."[37]. Europos žmogaus teisių teismas (EŽTT) yra atsakingas už šios konvencijos įgyvendinimą tarp 47 Europos Tarybos valstybių narių. Be to, asmenys gali kreiptis į EŽTT dėl žmogaus teisių pažeidimų, jei buvo išnaudotos visos

[35] Brendan Van Alsenoy, „Regulating data protection, the allocation of responsibility and risk among actors involved in personal data processing". Daktaro disertacija, Liuveno universitetas,2016. žiūrėta 2024m. gruodžio 3d. https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias1711667&context=SearchWebhook&vid=32KUL_KUL:Lirias&lang=en&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,LIRIAS1711667&offset=0

[36] „A Convention to protect your rights and liberties". Council of Europe, žiūrėta 2024m. gruodžio 3d. https://www.coe.int/en/web/human-rights-convention

[37] „Europos žmogaus teisių konvencija“, žiūrėta 2024m. gruodžio 3d. https://www.echr.coe.int/documents/d/echr/convention_eng

nacionalinės apeliacijos galimybės.[38] Nuo 1959 m. įkūrimo EŽTT priėmė daugiau nei 16 000 sprendimų, kurie turėjo reikšmingos įtakos Europos teisės aktams ir padėjo stiprinti teisės viršenybę šiame regione[39].

1981 m. priimta Konvencija dėl asmenų apsaugos automatizuotai tvarkant asmens duomenis, plačiai žinoma kaip Europos Tarybos 108 konvencija, laikoma vienu svarbiausių duomenų apsaugos dokumentų. Konvencija buvo priimta ir pasirašymui pateikta 1981 m., o įsigaliojo 1985 m. Nors iš pradžių ji buvo priimta regioniniu pagrindu, vėliau tapo tarptautine sutartimi. Tai įrodo ir tai, kad nuo 2013 m. konvenciją pradėjo ratifikuoti ne ES valstybės[40]. Konvencijos 108 tikslas buvo ne tiksliai apibrėžti privatumą ar asmens duomenis, o nustatyti tam tikrus apribojimus jautrių asmens duomenų tvarkymui. Šie apribojimai tapo būtini dėl vis didėjančio kompiuterių naudojimo organizacijų veikloje, kuris kėlė didelių iššūkių duomenų privatumui. Nors pirminiai 108 konvencijos privatumo principai išliko svarbūs ir laiko patikrinti, Europos Taryba pripažino būtinybę modernizuoti šį svarbų instrumentą. Modernizavimo procesas prasidėjo 2011 m. viešosiomis konsultacijomis, o 2018 m. gegužės 17–18 d. Danijoje vykusiame 128-ajame Europos Tarybos Ministrų komiteto posėdyje buvo priimtas pakeitimo protokolas (ETS Nr. 108). Po septynerių metų intensyvių diskusijų ir derybų 108 konvencija buvo atnaujinta 2018 m. gegužę. Šios modernizacijos tikslai buvo du: pirma, spręsti privatumo iššūkius, kylančius dėl naujų informacinių ir ryšių technologijų (IRT) naudojimo, ir, antra, stiprinti konvencijos įgyvendinimo mechanizmus[41].

Apibendrinant, konvencijos tikslas – *„užtikrinti, kad, tvarkant asmens duomenis automatizuotai, būtų gerbiamos kiekvieno asmens teisės ir pagrindinės laisvės, o svarbiausia – teisė į privatų gyvenimą. Protokole, kuriuo iš dalies keičiama Konvencija, siekiama išplėsti konvencijos taikymo sritį, padidinti duomenų apsaugos lygį ir veiksmingumą.“*[42]

BDAR yra vienas išsamiausių ir reikšmingiausių teisės aktų, reglamentuojančių duomenų apsaugą. Jis buvo patvirtintas 2016 m. balandžio 27 d. ir įsigaliojo 2018 m. gegužės 25 d. BDAR

[38] „The European Convention on Human Rights - how does it work?". Council of Europe, žiūrėta 2024m. gruodžio 3d. https://www.coe.int/en/web/impact-convention-human-rights/how-it-works

[39] „Landmark judgments". Council of Europe, žiūrėta 2024m. gruodžio 3d. https://www.coe.int/en/web/human-rights-convention/landmark-judgments

[40] „Chart of signatures and ratifications of Treaty 108“. Council of Europe, žiūrėta 2024m. gruodžio 3d. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

[41] „128th Session of the Committee of Ministers (Elsinore, Denmark, 17-18 May 2018) Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data“. Council of Europe, žiūrėta 2024m. gruodžio 3d. https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

[42] „Asmens duomenų apsauga, faktų apie Europos Sąjungą suvestinės“. Europos parlamentas, žiūrėta 2024m. gruodžio 3d. https://www.europarl.europa.eu/factsheets/lt/sheet/157/asmens-duomenu-apsauga

pakeitė Direktyvą 95/46/EB, įvesdamas naujas taisykles ir išplėsdamas jų taikymo sritį. Reglamento tikslas – užtikrinti, kad ES gyventojai galėtų kontroliuoti, kaip jų duomenys naudojami, ir sukurti aiškesnes taisykles verslui, siekiant užtikrinti saugų veikimą. BDAR numato griežtas baudas už jo nesilaikymą – iki 10 mln. eurų arba 2 proc. metinės apyvartos, priklausomai nuo to, kuri suma yra didesnė. BDAR taikymo sritis apima ne tik ES įmones, bet ir užsienio subjektus, kurie tvarko ES gyventojų duomenis[43].

BDAR svarba išryškėja dirbtinio intelekto (DI) kontekste, nes ši technologija itin plačiai naudoja asmens duomenis. Reglamento 4 straipsnyje pateikiamas platus asmens duomenų apibrėžimas apima tiek tiesioginius identifikatorius, tokius kaip vardas, pavardė, adresas, tiek netiesioginius, pavyzdžiui, IP adresus ar slapukų sugeneruotus identifikatorius. Tai tūrėtų užtikrinti, kad DI sistemų kūrėjai ir naudotojai privalėtų laikytis duomenų apsaugos principų.

Vienas iš BDAR principų – minimalus duomenų rinkimas, nurodantis, kad reikia rinkti tik tuos duomenis, kurie yra būtini konkrečiam tikslui pasiekti. Tai ypač svarbu DI algoritmams, kurie dažnai apdoroja didžiulius duomenų kiekius. Reglamento 5 straipsnis taip pat įpareigoja duomenų valdytojus veikti skaidriai, aiškiai informuojant duomenų subjektus apie jų duomenų tvarkymą. BDAR 22 straipsnis ypatingą dėmesį skiria automatizuotam sprendimų priėmimui ir profiliavimui, kuris dažnai naudojamas DI sistemose. Reglamentas suteikia asmenims teisę nebūti vien automatizuotų sprendimų, turinčių reikšmingą poveikį, objektu. Tai užtikrina asmenų apsaugą nuo diskriminacijos ar šališkų sprendimų, kurie gali kilti naudojant nepakankamai ištestuotus ar neobjektyvius algoritmus. Be to, BDAR reikalauja atlikti poveikio duomenų apsaugai vertinimą (35 straipsnis) tais atvejais, kai duomenų tvarkymas kelia didelę riziką asmenų teisėms ir laisvėms. Ši nuostata aktuali DI projektams, kurie apima jautrių ar didelio masto duomenų tvarkymą, pavyzdžiui, biometrinius ar sveikatos duomenis.

Nors BDAR svarba duomenų apsaugos kontekste yra neabejotina, šiame darbe jis nebus toliau detaliai analizuojamas. Ruošiant šį mokslinį darbą įvyko reikšmingi teisėkūros pokyčiai. Europos Sąjungoje buvo priimtas naujas teisės aktas, žinomas kaip Dirbtinio intelekto aktas. Kadangi šis teisės aktas yra pats naujausias teisinio reguliavimo reiškinys DI srityje, tolesnėje darbo dalyje pagrindinis dėmesys bus skiriamas būtent jo analizei. Bus aptarta šio akto reikšmė, taikymo sritys ir svarba, siekiant apsaugoti asmens teisę į privatumą sparčiai besivystančių DI technologijų kontekste.

[43] „supra note“

2021m. balandžio 21-ą dieną Europos Komisija pasiūlė dirbtinio intelekto akta ir 2024m. rugpjūčio 1-ą dieną šis aktas įsigalioja ir tampa pirmuoju pasaulyje teisės aktu, kuriuo reglamentuojamas dirbtinis intelektas. Toks reiškinys turi potencialo pavirsti pasauliniu DI reglamentavimo standartu, tokiu atveju istorija pasikartotų kaip ir su BDAR, kuomet reglamentas tapo standartu duomenų privatumo srityje.

Kaip nustatyta dirbtinio intelekto akte, *„šio reglamento paskirtis – pagerinti vidaus rinkos veikimą nustatant vienodą teisinę sistemą, visų pirma skirtą dirbtinio intelekto sistemų (toliau – DI sistemos) kūrimui, pateikimui rinkai, pradėjimui naudoti ir naudojimui Sąjungoje paisant Sąjungos vertybių, skatinti į žmogų orientuoto ir patikimo dirbtinio intelekto (toliau – DI) įsisavinimą kartu užtikrinant aukšto lygio sveikatos, saugumo, pagrindinių teisių, įtvirtintų Europos Sąjungos pagrindinių teisių chartijoje (toliau – Chartija), apsaugą, įskaitant demokratijos, teisinės valstybės ir aplinkos apsaugą, saugoti nuo žalingo DI sistemų poveikio Sąjungoje ir remti inovacijas. Šiuo reglamentu užtikrinamas laisvas DI grindžiamų prekių ir paslaugų tarpvalstybinis judėjimas, taip užkertant kelią valstybėms narėms nustatyti apribojimus DI sistemų kūrimui, teikimui rinkai ir naudojimui, nebent tai aiškiai leidžiama pagal šį reglamentą;*[44]*“* Europos sąjungos pagrindinių teisių chartijos 7 ir 8 straipsniai garantuoja teises į privatumą ir asmens duomenų apsaugą, todėl iš dirbtinio intelekto akto paskirties atsiskleidžia, kad šis aktas yra susijęs ir tinkamas teisės į privatumą kontekste.

Toliau šiame darbe išsamiau atliekama dirbtinio intelekto akto analizė per įvairias sritis – jo reikšmę, tikslus, rizikos klasifikaciją bei poveikį privatumo apsaugai, siekiant įvertinti, kaip šis teisinis reguliavimas prisideda prie asmens teisės į privatumo apsaugos užtikrinimo ir ar šis aktas gali prisidėti prie grėsmių mažinimo.

Pagrindinis akto tikslas sukurti teisinį pagrindą, kurio remiantis būtų užtikrinamas toks DI technologijų vystymasis, kuris nepažeistų pamatinių žmogaus teisių ir tarnautų visuomenės gerovei. Šis aktas ne tik įpareigoja DI sistemų kūrėjus ir naudotojus laikytis tam tikrų normų, bet ir nubrėžia aiškias ribas, kuriais atvejais jų peržengti negalima. Kad tos ribos būtų aiškios DI sistemos akte yra grupuojamos į skirtingo lygio rizikas.

Griežčiausiai vertinamos sistemos, kurių naudojimas yra uždraustas, skiriamos į nepriimtinos rizikos grupę. Tokios sistemos kelia grėsmę žmogaus teisėms, laisvėms ir demokratiniams procesams. DI aktu draudžiamos aštuonios praktikos rūšys:

[44] „Dirbtinio intelekto aktas“, žiūrėta 2024m. gruodžio 3d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=OJ:L_202401689

1) žalingas dirbtiniu intelektu grindžiamas manipuliavimas ir apgaulė. Realus pavyzdys „Deepfake“ technologija. „Deepfake“ – tai terminų „gilus mokymasis“ (angl. deep learning) ir „klastotė“ (angl. fake) junginys. Deepfake yra ypač realistiški vaizdo įrašai, kurie skaitmeniniu būdu manipuliuojami taip, kad juose esantys asmenys atrodytų sakantys ar darantys dalykus, kurie realybėje niekada neįvyko. Šios technologijos pagrindas – dirbtinių neuroninių tinklų naudojimas, analizuojant didelius duomenų rinkinius, kad būtų išmokta imituoti asmens veido išraiškas, manieras, balsą ir intonacijas. Procesas apima dviejų žmonių vaizdo įrašų pateikimą giluminio mokymosi algoritmui, kuris išmoksta keisti vieno asmens veidą kitu.[45] Šia technologija sukurtų vaizdo įrašų dažnai galima pamatyti įvairiose socialiniuose tinkluose, kuomet yra padirbamos įvairių politikų, visuomenės veikėjų kalbos.

2) žalingas dirbtiniu intelektu grindžiamas pažeidžiamumų išnaudojimas. Tokia praktika gali būti naudojama nusikaltėlių, kurie gal būt neturėdami pakankamo raštingumo, pasinaudoja kalbos modeliais, pavyzdžiui „CHAT GPT“ kurdami įtikinamus, profesionalius laiškus, apsimetant banko ar kitų institucijų darbuotojais ir stengiasi išvilioti iš asmens tam tikrus duomenis arba pinigus.

3) socialinis vertinimas balais. Realus pavyzdys pasaulyje Kinijos vykdoma socialinio reitingavimo sistema, kurioje piliečiai realiai skirstomi į „gerus“ ir „blogus“[46], gauna ar praranda balus priklausomai nuo savo elgesio. Aukštesni balai suteikia galimybes, pvz., lengvesnes paskolas ar greitesnes vizas, o žemesni – gali apriboti galimybę keliauti ar gauti valstybės paslaugas.

4) Atskirų nusikalstamų veikų rizikos vertinimas arba prognozavimas. Jungtinėse Valstijose buvo naudojama COMPAS - Correctional offender management profiling for alternative sanctions sistema, kuri įvertina kalinių tikimybę vėl nusikalsti. Praktika parodė, kad ši sistema turėjo šališkumų prieš afroamerikiečius, nes jie dažniau buvo vertinami kaip keliantys daugiau rizikos nusikalsti, lyginant su baltaodžiais.[47]

5) netikslinis interneto ar apsauginės vaizdo stebėjimo sistemos medžiagos rinkimas siekiant sukurti arba išplėsti veido atpažinimo duomenų bazes. Realių pavyzdžių, kuomet buvo naudojamos tokios sistemos, istorijoje jau turime. Clearview AI rinko didelius kiekius veidų nuotraukų iš įvairių

---

[45] Mika Westerlund, „The Emergence of Deepfake Technology: A Review“. *Technology innovation management review* (2019): 1-14, žiūrėta 2025m. kovo 14d. https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf

[46] Rui Hou, Diana Fu, „Sorting citizens: Governing via China's social credit system“, žiūrėta 2025m. kovo 14d. https://www.researchgate.net/profile/Rui-Hou 2/publication/365862623_Sorting_citizens_Governing_via_China%27s_social_credit_system/links/6464f64a702026631653fff0/Sorting-citizens-Governing-via-Chinas-social-credit-system.pdf

[47] Goda Strikaitė-Latušinskaja „Automatizuoti administraciniai nurodymai Lietuvoje“. *Teisė* (2022):, žiūrėta 2025m. kovo 14d. https://www.zurnalai.vu.lt/teise/article/download/30836/29758?

socialinių tinklų, svetainių, kurdama didžiausią pasaulyje veido atpažinimo duomenų bazę, tačiau, net dar neegzistuojant dirbtinio intelekto aktui, tokios sistemos kūrimas jau pažeidė tam tikrus įstatymus, pavyzdžiui BDAR nustatytas normas. Pagrindinė to priežastis, didžioji dalis žmonių nežinojo, kad jų veidai traukiami į sistemą.[48]

6) emocijų atpažinimas darbo vietose ir švietimo įstaigose. Technologijų ir dirbtinio intelekto dėka egzistuoja prietaisai, pavyzdžiui, matuojantys mokinio smegenų veiklą ir emocinę būseną pamokų metu, tačiau tai kelia susirūpinimą dėl asmens privatumo, psichologinės įtampos, todėl tokių sistemų įtraukimas į draudžiamų praktikų sąrašą atrodo pagrįstas ir reikalingas.

7) biometrinis skirstymas į kategorijas siekiant nustatyti tam tikras saugomas savybes. Tokios sistemos skirtos žmonių grupavimui pagal jų biologines ar fizines savybes, siekiant nustatyti tam tikrus požymius, rasę, lytį, amžių, sveikatos būklę.

8) Realiu laiku vykstantis nuotolinis biometrinis tapatybės nustatymas teisėsaugos tikslais viešosiose erdvėse. Tokios sistemos realiu laiku gali atpažinti asmenį nuskaitant jo veidą, kas gali padėti aptikti ieškomus asmenis, tačiau tuo pačiu yra masiškai stebimi asmenys ir jų asmenybės yra nustatomos, nors jie nėra susiję su nusikalstamomis veikomis, todėl tai pažeidžia jų privatumą.

Be nepriimtinos rizikos sistemų, taip pat yra išskiriamas ir didelės rizikos sistemų sąrašas, kurios nebus draudžiamos, tačiau griežtai reguliuojamos. Tokios sistemos susijusios su sveikata, sauga, pagrindinėmis asmens teisėmis. Didelės rizikos naudojimo atvejus apima:

1) DI saugos sistemos, atsakingos už svarbius infrastruktūros objektus. Pavyzdžiui – DI sistemų naudojimas transporto saugumo sistemose, kurių gedimas būtų pavojingas žmogaus sveikatai ar gyvybei.

2) DI sistemos švietime, pavyzdžiui automatinio egzaminų vertinimo sistema, tokia sistema gali turėti įtakos žmogaus būsimai karjerai, jo planuojamai ateičiai.

3) DI medicinoje, tokių sistemų naudojimas tikrai kelia didelę riziką, kadangi jų netikslumas, pavyzdžiui chirurgijoje, gali turėti rimtų pasėkmių.

4) DI įdarbinimo ir darbo veiklos sistemos. Vienas iš pavyzdžių „HireVue“ sistema, kuri padeda darbdaviui taupyti laiką ir kandidatus, norinčius įsidarbinti analizuoja pagal jų veido išraiškas, kalbos manieras, balsą taip filtruodama tinkamus ir netinkamus darbuotojos darbdaviui.[49]

---

[48] „Facial recognition: Italian SA fines Clearview AI EUR 20 million“. European data protection board, žiūrėta 2025m. kovo 18d., https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

[49] „A face-scanning algorithm increasingly decides whether you deserve the job”. The Washington post , žiūrėta 2025m. kovo 18d. https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/

5) DI naudojimas kasdienėse paslaugose, pavyzdžiui DI gali neobjektyviai įvertinti žmogaus kreditingumą, kas gali lemti ar jam bus suteikta būsto paskola, tokios sistemos sprendimas gali turėti didelę įtaką žmogaus gyvenimui.

6) DI naudojamas nuotoliniam žmonių atpažinimui, tapatybės nustatymui, biometriniam skirstymui, emocijų atpažinimui.

7) Sistemų naudojimas teisėsaugos srityse, pavyzdžiui analizuoti įrodymus teismuose.

8) Naudojimas migracijos ir sienų kontrolės srityse, pavyzdžiui automatizuotos sistemos, kurios nagrinėja migrantų duomenis ir vizų prašymus.

9) DI sprendimai teismų procesuose, sistemos, kurios padeda teisėjams rengti sprendimus taip pat vertinamos kaip didelės rizikos sistemos.

Analizuojant šias dvi rizikos grupes, aišku, kad nepriimtinos DI sistemos yra visiškai draudžiamos, nes jos kelia tiesioginę grėsmę žmogaus teisėms, demokratijai, visuomenės saugumui. Tačiau didelės rizikos sistemos leidžiamos naudoti pasitelkiant griežtą kontrolę. Šis skirtumas rodo, kad Europos Sąjungos DI aktas siekia ne tik užkirsti kelią grėsmingoms sistemoms, tačiau tuo pačiu siekia sukurti aiškų reguliavimą, kuris taip pat leistų ir inovacijas, kartu apsaugant žmonių teises. Be šių dviejų stipriai kontroliuojamų rizikos rūšių, taip pat išskiriamos ir skaidrios rizikos sistemos, pavyzdžiui, pokalbių robotai, tokioms sistemoms pagrindinis reikalavimas yra pranešimas naudotojui, kad šis bendrauja ir sąveikauja su mašina, dirbtinio intelekto sistema. Minimalios rizikos sistemoms, pavyzdžiui, brukalų filtrams, vaizdo žaidimams, dirbtinio intelekto akte nenustatytos jokios taisyklės.

Šių laikų kontekste DI akto išleidimas turi didelę reikšmę. Visų pirma Europos Sąjunga tampa pirmaujančia jurisdikcija, kuri nustatė DI etikos ir saugumo standartus, kuriuos ilgalaikėje perspektyvoje gali perimti ir kitos šalys. Taip pat šis aktas apsaugo piliečių teises dirbtinio intelekto kontekste, nustatydamas aiškias kūrimo ir naudojimo gaires. Dar vienas svarbus aspektas, juridiniams asmenims sukuriamas teisinis aiškumas, kuris padės įmonėms vystyti DI technologijas, žinant aiškias ribas.

Nepaisant to, kad DI aktas yra turinti daug potencialo Europos sąjungos iniciatyva, siekiant rezultatų gali kilti ir įvairūs iššūkiai. Vienas iš pagrindinių subjektų, kuriems bus taikomas šis aktas, yra DI sistemų kūrėjai, todėl realu, kad iš verslo ir technologijų sektoriaus gali kilti reakcijos, argumentuojančios, kad griežtas reguliavimas stabdo inovacijas, tokiu atveju iššūkis Europos Sąjungai yra rasti bendrą kalbą su kūrėjais ir siekti abiejų pusių bendradarbiavimo. Be to, atsižvelgiant į spartų technologijų vystymąsi , jų kintančius veikimo principus, įsigaliojus DIA, nors aktas ir detaliai reglamentuoja aukštų rizikų DI sistemas, svarbus nuolatinis stebėjimas ir atnaujinimai realiu laiku

esant pokyčiams, tam, kad išvengti teisinių spragų naudojimo. Taip pat svarbus aspektas praktinis įgyvendinimas, didelis iššūkis laukia Europos Sąjungos valstybių, kurios turės užtikrinti, kad DI aktas bus efektyviai taikomas ir nebus apeinamas.

Apibendrinant, DI aktas žymi vieną iš pirmųjų ne tik teorinių, bet ir praktinių bandymų reguliuoti dirbtinį intelektą, nubrėžiant aiškias taisykles ir sukuriant precedentą, kuris gali įtakoti kitas valstybes, kurios svarsto apie savo DI reguliavimą. Akto pagrindas yra rizikos klasifikacija, kas atrodo aišku ir logiška, tačiau klausimas, ar šis aktas veiks praktiškai, lieka atviras ir pamatyti rezultatus praktikoje reikės laiko, atsižvelgiant ir į tai, kad visapusiškai aktas taikomas bus nuo 2026m. rugpjūčio 2d., su išimtimis tam tikroms taisyklėms ir iki 2027m. rugpjūčio 2d. Praktika parodys, ar nepriimtinų sistemų uždraudimas bus veiksmingas, ar bus užtikrinta, kad tokios sistemos nebus naudojamos slaptai arba apeinant teisės aktus. Atkreiptinas dėmesys, kad atlikus DI akto analizę ir jau išnagrinėjus privatumo sampratą, toliau darbe bus galima išnagrinėti ir atskleisti, kokios konkrečios grėsmes kyla vartotojui naudojant dirbtinį intelektą jo teisėms į privatumą, nes būtent DI akto analizė leidžia suprasti, kokios privatumo sritys yra ginamos DI kontekste ir kur kyla rizikos.

3.2 Nacionalinių teisės aktų ir priemonių analizė

Toliau darbe nagrinėjami nacionaliniai teisės aktai ir priemonės, kurių imasi Lietuvos Respublikos valstybinės institucijos, asmens teisių į privatumą saugumui užtikrinti. Atliekant šią analizę, pirmiausia buvo nagrinėtas svarbiausias nacionalinis teisės aktas- Lietuvos Respublikos Konstitucija. Konstitucijos 22 straipsnis nusako, kad žmogaus privatus gyvenimas neliečiamas, 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 orumą.[50] Lietuvos Respublikos Konstitucija buvo priimta referendumu 1992m. spalio 25d. , tuo metu dirbtinio intelekto technologija Lietuvoje dar nebuvo pakankamai išplėtota ir nebuvo tokia aktuali tema kaip šių dienų visuomenėje, todėl joje dirbtinio intelekto sąvokos nėra. Lietuvos Respublikos Konstitucinio teismo 1991m. sausio 31d. nutarime teisė į privatumą aiškinama taip – „*Šiame Konstitucijos straipsnyje įtvirtintos normos gina asmens teisę į privatumą. Ši teisė apima privatų, šeimos ir namų gyvenimą, asmens fizinę ir psichinę*

[50] Lietuvos Respublikos Konstitucija, žiūrėta 2025m. kovo 26d.

neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kt. Savavališkai ir neteisėtai kišantis į žmogaus privatų gyvenimą kartu yra kėsinamasi į jo garbę bei orumą.“[51] Nors nei straipsnyje, nei teismo aiškinime nenurodytos sąsajos su dirbtiniu intelektu, manytina, kad 22 straipsnio nuostatų kontekstą galima sieti su dirbtinio intelekto keliamomis grėsmėms asmens privatumui. Pavyzdžiui, savavališku ir neteisėtu kišimusi į privatų gyvenimą laikytinas neteisėtas, be asmenų sutikimo, DI sistemų naudojimas , kurios gali masiškai rinkti ir analizuoti asmeninius duomenis. DI sistemų naudojimas profiliavimui, kelia grėsmę asmenų psichinei neliečiamybei. Profiliavimas – bet kokios formos automatizuotas asmens duomenų tvarkymas, kai asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti ar numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu.[52] Šio straipsnio kontekste galima įžvelgti gynybos ir kitoms grėsmėms kaip šeimos ir namų gyvenimo privatumui, kuomet išmanieji įrenginiai su DI sistemomis gali tapti priemonėmis nelegaliam sekimui, be to netinkamai apsaugotas DI sistemų naudojimas gali nutekinti privačius duomenis, pavyzdžiui iš sveikatos įstaigų, tokie veiksmai tiesiogiai pažeistų draudimą skelbti konfidencialią informaciją.

Bendruoju požiūriu teisė į privatumą reglamentuojama ir Lietuvos Respublikos baudžiamajame kodekse. Teisei į privatumą LRBK išskiriamas atskiras skyrius ir šie straipsniai - 165 Straipsnis. Neteisėtas asmens būsto neliečiamumo pažeidimas, 166 Straipsnis. Asmens susižinojimo neliečiamumo pažeidimas, 167 Straipsnis. Neteisėtas informacijos apie privatų asmens gyvenimą rinkimas, 168 Straipsnis. Neteisėtas informacijos apie asmens privatų gyvenimą atskleidimas ar panaudojimas.[53]

Lietuvos Respublikos darbo kodekso 27 straipsnis su dirbtinio intelekto reguliavimu siejasi glaudžiau, kadangi šio straipsnio antroje dalyje įtvirtinta nuostata, jog darbdavys, įgyvendinamas nuosavybės ar valdymo teises į darbo vietoje naudojamas informacines ir elektroninių ryšių technologijas, negali pažeisti darbuotojų asmeninio susižinojimo slaptumo. Atsižvelgiant į spartų DI technologų plėtra, ši darbo kodekso norma tampa aktuali sprendžiant automatizuoto duomenų stebėjimo ir privatumo apsaugomus klausimus darbo santykių kontekste.

[51] „Dėl Lietuvos Respublikos Aukščiausiosios Tarybos 1991 m. sausio 31 d. nutarimo „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase“ atitikimo Lietuvos Respublikos Konstitucijai" LR Konstitucinio teismo nutarimas, žiūrėta 2025m. kovo 31d.
[52] „supra note“, žiūrėta 2025m. kovo 31d.
[53] „Lietuvos Respublikos baudžiamasis kodeksas“, žiūrėta 2025m. kovo 31d.

Iš analizuotų nacionalinių teisės aktų galima teigi, kad Lietuvos Respublikos Konstitucijos, baudžiamojo bei darbo kodeksų nuostatos nėra sukurtos konkrečiai dirbtinio intelekto kartu su teise į privatumą reguliavimui, tačiau šios normos leidžia daryti prielaidas, jog tam tikrais atvejais jos gali būti taikomos ir DI keliamų iššūkių kontekste. Tęsiant nacionalinių teisės aktų analizę, pastebėtina, kad šiuo metu Lietuvos Respublikos teisinėje sistemoje nenustatyta specialaus teisės akto, kuris tiesiogiai reglamentuotų dirbtinio intelekto keliamų grėsmių asmens teisėms į privatumą apsaugą. Nepaisant to, atkreiptinas dėmesys, kad valstybinės institucijos aktyviai siekia įgyvendinti Europos dirbtinio intelekto akto nuostatas. Todėl toliau bus analizuojamos Lietuvos institucijų iniciatyvos ir veiksmai, kuriais siekiama pasiruošti ir įgyvendinti DI aktą Lietuvos Respublikoje.

LR Ekonomikos ir inovacijų ministerijos šaltiniuose pateikiami šie Lietuvos Respublikos pagrindiniai įsipareigojimai – paskelbti žmogaus teises ginančių institucijų sąrašą, parengti taisykles dėl leidimų naudoti realaus laiko nuotolinio biometrinio tapatybės nustatymo sistemą teisėsaugos tikslais, paskirti nacionalines kompetentingas institucijas, parengti taisykles dėl sankcijų taikymo, sukurti DI reguliacines smėliadėžes ir parengti gaires jų dalyviams, įgyvendinti teisę pateikti skundą rinkos priežiūros institucijai, parengti taisykles, pagal kurias galima susipažinti su DI sistemos tiekėjo privalomais saugoti dokumentais, net jei jis nutraukia savo veiklą. Šie pagrindiniai įsipareigojimai planuojami įgyvendinti iki 2027-08-02. Lietuvos Respublikai vykdant įsipareigojimus, lygiagrečiai įsipareigojimus turės vykdyti ir DI sistemų tiekėjai. [54]

Lietuvos Respublika tam tikrus įsipareigojimus yra jau įvykdžiusi, pavyzdžiui, yra paskelbtas žmogaus teises ginančių institucijų sąrašas. Šios institucijos yra svarbiausios ginant žmogaus teises Lietuvoje naudojant didelės rizikos DI sistemas.

1) Lygių galimybių kontrolieriaus tarnyba – svarbiausias institucijos tikslas užtikrinti, kad privatūs ir vieši asmenys nepažeistų asmenų lygiateisiškumo principo ir laikytųsi diskriminacijos draudimo.

2) Seimo kontrolierių įstaiga – ši institucija atlieka žmogaus teisių stebėseną Lietuvoje, taip pat inicijuoja tyrimus dėl esminių žmogaus teisių problemų, vykdo sklaidą ir visuomenės švietimą žmogaus teisių klausimais.

3) Vaiko teisių apsaugos kontrolieriaus įstaiga – šios įstaigos paskirtis gerinti vaiko teisinę apsauga, ginti vaiko teises ir jo teisėtus interesus.

[54] „Laiko juosta- DI akto įsigaliojimas ir pagrindiniai įsipareigojimai“. LR Ekonomikos ir inovacijų ministerija , žiūrėta 2025m. balandžio 7d. https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/laiko-juosta/

4) Žurnalistų etikos inspektoriaus tarnyba – tiria žmogaus teisių pažeidimus visuomenės informavimo priemonėse.

Šios įstaigos, remiantis DI akto 77str. turi teisę – prašyti prieigos ir gauti visus pagal DI aktą saugomų dokumentus, susijusius su didelės rizikos DI sistemų naudojimu, teikti prašymus rinkos priežiūros institucijai, kad ji organizuotų didelės rizikos DI sistemos bandymą, jeigu gautų dokumentų nepakanka įsitikinti, kad nebuvo pažeisti ES Teisės aktai dėl žmogaus teisių apsaugos. Taip pat šiame sąraše pateiktos įstaigos turi pareigą – informuoti rinkos priežiūros instituciją apie bet kokį pateiktą prašymą dėl prieigos prie saugomų dokumentų, bendradarbiauti su RPO , laikytis DI akto 78str. nustatytų konfidencialumo reikalavimų.[55]

Taip pat buvo analizuojamas ir bendras nacionalinių priemonių sąrašas, šios priemonės padės valstybei įgyvendinti nustatytus reikalavimus, kuriuos privalo įgyvendinti visos valstybės narės. Sąraše viso pateikiama šešiolika priemonių, toliau išskiriamos trys, kurios vertinamos kaip reikšmingiausios[56]:

1) Lietuvos Respublikos technologijų ir inovacijų įstatymo Nr. XIII-1414 1, 2, 11, 13, 14, 17, 21 straipsnių pakeitimo ir įstatymo papildymo priedu įstatymo projektas. Projekto tikslas – paskirti viešąją įstaigą Inovacijų agentūrą nacionaline kompetentinga institucija – notifikuojančiąja institucija, taip pat nustatyti, kad viešoji įstaiga Inovacijų agentūra būtų atsakinga už apribotos bandomosios dirbtinio intelekto reglamentavimo aplinkos sukūrimą ir šios aplinkos veikimo priežiūrą. Ši priemonė išskiriama kaip svarbi dėl to, kad institucijų koordinavimas yra būtinas siekiant užtikrinti sklandų bendradarbiavimą tarp valstybių narių bei tarp nacionalinių ir ES institucijų.

2) Lietuvos Respublikos informacinės visuomenės paslaugų įstatymo Nr. X-614 1, 2, 23 straipsnių ir priedo pakeitimo įstatymo projektas. Projekto tikslas – paskirti Lietuvos Respublikos ryšių reguliavimo tarnybą nacionaline kompetentinga institucija – rinkos priežiūros institucija, taip pat pavesti jai atlikti bendro kontaktinio punkto funkcijas. Dėl šio projekto įgyvendinimo Lietuvos Respublikos ryšių reguliavimo tarnybą tapo kertiniu subjektu, atsakingu už technologijų priežiūrą, skaidrumą ir atitikį reikalavimams.

3) Dirbtinio intelekto taikymo ir priežiūros įstatymo projektas. Projekto tikslai: nustatyti taisykles dėl sankcijų ir kitų vykdymo užtikrinimo priemonių, kurios taip pat gali apimti įspėjimus ir

[55] „Žmogaus teises ginančių institucijų sąrašas“. LR Ekonomikos ir inovacijų ministerija, žiūrėta 2025m. balandžio 7d. https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/zmogaus-teises-ginancios-istaigos/

[56] „Bendras nacionalinių priemonių sąrašas“. LR Ekonomikos ir inovacijų ministerija, žiūrėta 2025m. balandžio 7d. https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/nacionaliniu-priemoniu-sarasas/

nepinigines priemones, taikytinų už veiklos vykdytojų padarytus šio reglamento pažeidimus, ir imtis visų būtinų priemonių užtikrinti, kad jos būtų tinkamai ir veiksmingai įgyvendinamos. Nustatyti funkcijų pasiskirstymą tarp DI sistemų rinkos priežiūrą atliekančių institucijų (nacionalinės kompetentingos institucijos ir kitų priežiūros institucijų). Šio projekto įgyvendinimas užtikrins sankcijų ir vykdymo užtikrinimo mechanizmus bei aiškų institucijų, atliekančių priežiūrą, funkcijų paskirstymą.

Apibendrinant nacionalinių teisės aktų analizę galima teigti, kad nors šiuo metu Lietuvos Respublikos teisinėje sistemoje nėra specialaus dirbtinio intelekto technologijų keliamos rizikos asmens privatumui reglamentuojančio teisės akto, nacionaliniai teisės aktai, tokie kaip LR Konstitucija, Baudžiamasis, Darbo kodeksai, jau dabar sudaro teisinį pamatą tam tikriems DI naudojimo atvejams analizuoti ir vertinti privatumo apsaugos aspektais. Tačiau šios normos nėra pakankamai konkrečios ar išsamios, kad jas būtų galima taikyti savarankiškai kylant teisinėms problemoms DI kontekste.

Dėl šios priežasties siekis įgyvendinti Europos Sąjungos dirbtinio intelekto aktą tampa ypač svarbus, Lietuvos valstybės institucijų inciatyvos ir reikalavimų vykdymas šiame kontekste tampa ypač pozityviu rodikliu. Nacionalinių teisinių priemonių ir institucinių struktūrų formavimas yra svarbus žingsnis siekiant parengti Lietuvą efektyviam dirbtinio intelekto reglamentavimui. Autoriaus nuomone, apibendrinant, galiojantis reglamentavimas vis dar atsilieka nuo technologinės pažangos, o tai kelia riziką žmogaus teisėms būti sistemingai pažeidžiamoms, todėl ypač svarbu sutelkti dėmesį į greitą ir sklandų Europos Sąjungos dirbtinio intelekto akto įgyvendinimą praktikoje.

4. DIRBTINIO INTELEKTO TECHNOLOGIJŲ TAIKYMO POVEIKIS ASMENS TEISĖS Į PRIVATUMĄ APSAUGAI. PRAKTINIŲ ATVEJŲ ANALIZĖ

Siekiant išsamiai ir nuodugniai atskleisti dirbtinio intelekto poveikį asmens teisei į privatumą, šiame darbe atliekamas kokybinis tyrimas, naudojant atvejo analizės (anglų k. case study) metodą. Toks metodas pasirinktas todėl, kad kiekybiniai metodai, kaip apklausa ar statistinė analizė, šio darbo kontekste nėra tinkami, nes analizuojamas reiškinys pirmiausia yra labai naujas ir susijęs su kompleksiškai teisinėmis, etinėmis ir technologinėmis sritimis. Tokį sprendimą lėmė ir kita objektyvi priežastis. Visų pirma, analizuojant Europos Žmogaus Teisių Teismo praktiką ir įvairių valstybių nacionalinių teismų sprendimus paaiškėjo, kad tiesiogiai su dirbtinio intelekto sistemų sukeltomis grėsmėmis privatumui susijusių teismų sprendimų yra labai mažai. Dažniausiai dirbtinio intelekto

kontekstas minimas tik netiesiogiai, o konkrečiai įvardytų ir išspręstų teisminių ginčų, susijusių su DI įtakos asmens duomenų apsaugai klausimais, kol kas beveik nėra. Dėl šių priežasčių teismų praktikos analizė kaip tyrimo metodas šiuo atveju pasirodė neefektyvi ir nepakankama, siekiant atskleisti realią dirbtinio intelekto technologijų įtaką privatumo teisių apsaugai.

Kokybinių tyrimų skiriamųjų bruožų analizė, atlikta remiantis įvairiais šaltiniais, leidžia jį apibūdinti kaip sistemingą, nestruktūrizuotą atvejo ar individų grupės, situacijos ar įvykio tyrimą natūralioje aplinkoje, siekiant suprasti tiriamuosius reiškinius bei pateikti interpretacinį, holistinį jų paaiškinimą.

Kiekybinių ir kokybinių tyrimų skirtumai. Skirtingai nuo kokybinių, kiekybiniam tyrimui labiau būdingas siekis ieškoti išorinių reiškinio požymių, išgaunant įvairius rodiklius, kurie gali būti išreikšti skaičiais ir matuojami. Todėl kiekybinio tyrimo mokslinę vertę nusako gauti jo rezultate kiekybiniai rodikliai. Be to, kiekybinis tyrimas yra labiau struktūrizuotas ir suplanuotas, nes tyrimo metodai bei duomenų matavimo priemonės dažniausiai būna sukonstruotos dar prieš tyrimą. Tuo tarpu kokybinių tyrimų metodai yra lankstūs, nes orientuoti į interpretaciją, o ne į matavimus; į procesą, o ne į išvadą; sutelkia dėmesį į situacijos ir elgesio ryšį, kuris daro didžiausią įtaką patirties formavimui. Be to, skirtingai negu kiti, kokybiniai tyrimo metodai labiau gilinasi į daiktų ir reiškinių kilmę, o ne į skaičius.[57]

Tyrime pasirinktas atvejo analizės metodas leidžia nuosekliai ir detaliai išnagrinėti atskirus įvykius, susijusius su dirbtinio intelekto technologijų taikymu ir jų poveikiu žmogaus teisėms į privatumą. Šis metodas pasirinktas dėl to, kad jį taikant galima išsamiai ištirti ir suprasti konkrečius teisės į privatumą pažeidimus, kurie įvyko dėl dirbtinio intelekto naudojimo, taip suteikiant praktinį pagrindą giliau analizuoti šią temą.

Atvejo studija (angl. Case study) suteikia galimybę nuodugniai išanalizuoti ir aprašyti vieną įvykį ar faktą realiame kontekste ir aprašyti (paaiškinti) tiriamą reiškinį, ypač, kai tarp reiškinio ir jo konteksto ribos nėra aiškios. Atvejo studija dažniausiai susideda iš informacijos surinkimo ir analizės etapų. Atvejo studijos gali būti naudojamos formuluojant teorijas arba siekiant aprašyti (pvz. išsamiai atskleisti organizacijos gerąją patirtį, siekiant iliustruoti ar paaiškinti tam tikrą fenomeną ar tendenciją). Atvejo studijoms gali būti naudojami tiek kiekybiniai, tiek ir kokybiniai duomenys.
Atvejo studija yra gana plačiai naudojama organizacijų veiklos studijose ir visose socialinių mokslų srityse. Pastaraisiais metais pastebima atvejo analizės, kaip mokslinio tyrimo metodo pozicijų

[57] K. Kardelis, „Mokslinių tyrimų metodologija ir metodai“ Kaunas: Mokslo ir enciklopedijų leidybos centras,2002. žiūrėta 2025m. balandžio 10d. https://verslas09.wordpress.com/wp-content/uploads/2010/01/mtp.pdf

stiprėjimo tendencija, vis dažniau atvejo analizė naudojama kaip patikima mokslinių tyrimų strategija (Hartley, 1994, 2004, Stake, 2000). Nors metodas nėra nei naujas nei savo esme grynai kokybinis tyrimas, atvejų studija tampa viena iš labiausiai paplitusių būdų, skirtų kokybinių tyrimų atlikimui. Tai tokia kokybinių tyrimų strategija, kai detaliai, giliai nagrinėjamas vienas ar keli konkretūs atvejai, iliustruojantys tiriamąją problemą. Čia didžiausias dėmesys skiriamas konkrečiam atvejui, kurį bandoma kuo išsamiau aprašyti ir paaiškinti bei atsakyti į tyrimo klausimus.[58]

Pasirinkti konkretūs atvejai – „Clearview AI“ bei „Cambridge Analytica“ – yra neatsitiktiniai. Jie abu tiesiogiai ir plačiai žinomi visuomenei bei susiję su reikšmingais teisės į privatumo pažeidimais, įvykdytais naudojant dirbtinio intelekto technologijas. Šių dviejų atvejų analizė leidžia ne tik atskleisti specifines grėsmes, kylančias privatumo apsaugai dėl dirbtinio intelekto taikymo, bet ir formuluoti rekomendacijas bei įžvalgas, kurios gali būti naudingos kuriant ir tobulinant teisinį reguliavimą šioje srityje. Pasirinkti atvejai taip pat puikiai iliustruoja teoriniuose skyriuose analizuotų teisinių ir technologinių aspektų svarbą bei aktualumą praktinėje erdvėje, todėl atvejo analizė šiame darbe bus naudinga siekiant išsamių ir praktiškai pagrįstų išvadų.

Clearview AI atvejis pasirinktas, nes ši įmonė taikė veido atpažinimo technologiją, pagrįstą dirbtiniu intelektu, neteisėtai rinkdama milijonų žmonių biometrinius duomenis iš viešų interneto šaltinių, socialinių tinklų ir kitų platformų. Šis atvejis leidžia atskleisti specifinius pavojus, kuriuos kelia automatizuotas, masinis biometrinių duomenų rinkimas ir apdorojimas dirbtinio intelekto pagalba.

Cambridge Analytica atvejis yra svarbus dėl to, kad jis atskleidžia, kaip dirbtiniu intelektu pagrįstos profiliavimo ir duomenų analizės sistemos gali būti naudojamos ne tik komerciniais, bet ir politiniais tikslais, manipuliuojant asmenimis ir jų privatumu. Šis atvejis taip pat leidžia giliau pažvelgti į psichologinio profiliavimo bei manipuliavimo asmenų duomenimis problematiką.

4.1 Clearview AI atvejo analizė

Pirmiausia bus nagrinėjamas plačiai žinomas ir reikšmingas „Clearview AI“ atvejis, kuris atskleidžia, kaip dirbtinio intelekto technologijos, ypač biometrinių duomenų atpažinimo sistemos, gali tiesiogiai paveikti asmenų teisę į privatumą. „Clearview AI“ technologija sukėlė daug diskusijų ir teisinių ginčų dėl savo kontraversiško veikimo principo – milžiniškų asmens duomenų kiekių

[58] „Tyrimų metodai ir metodikos“. Mokslo medis , žiūrėta 2025m. balandžio 10d. https://mokslomedis.lt/atvejo-studija/

rinkimo iš įvairių šaltinių internete be vartotojų sutikimo. Šios analizės tikslas – detaliai išnagrinėti šio atvejo faktines aplinkybes, identifikuoti pagrindinius teisės į privatumo pažeidimus, įvertinti esamo teisinio reguliavimo efektyvumą bei pateikti išvadas apie šio įvykio reikšmę dirbtinio intelekto reguliavimo kontekste.

Oficialiame įmonės tinklalapyje „Clearview AI“ aprašoma kaip privati Jungtinėse Amerikos Valstijose įsikūrusi įmonė, kurios siekis kurti pažangiausias technologijas ir jas teikti teisėsaugos institucijoms, vyriausybinėms organizacijoms bei kariuomenei, kurių tikslas padėti tirti nusikaltimus, stiprinti visuomenės saugumą, užtikrinti bendruomenių apsaugą ir siekti teisingumo nusikalstamų veikų aukoms. Ši platforma yra paremta veido atpažinimo technologija, turinti daugiau nei 50 milijardų veido atvaizdų duomenų bazę. Duomenų bazė yra renkama iš viešai prieinamų internetinių šaltinių, tokių kaip naujienų portalai, paieškomų asmenų svetainės, vieši socialinių tinklų profiliai ir kiti atviri šaltiniai. Įmonės manymu, jų sprendimai suteikia galimybę įvairioms institucijoms gauti žvalgybinę informaciją, kovoti su nusikalstamumu ir stiprinti visuomenės saugumą, galutinis įmonės tikslas – stiprinti pareigūnų ir visuomenės saugumą bei užtikrinti bendruomenių ir šeimų gerovę.[59]

Atsižvelgiant į oficialų „Clearview AI“ pateikiamą aprašymą, galima apibendrinti pagrindinius šios technologijos aspektus:

1) „Clearview AI“ yra privati Jungtinių Amerikos Valstijų įmonė.

2) Technologija skirta – teisėsaugai, vyriausybinėms institucijoms, kariuomenėi.

3) Technologija veikia kaip veido atpažinimo platforma, paremta viešai prieinamais duomenimis.

4) Duomenų bazės apimtis – daugiau nei 50 milijardų vaizdų.

5) Paskirtis – nusikaltimų tyrimas, saugumo stiprinimas, teisingumas aukoms.

4.1.1 Faktinės atvejo aplinkybės

2020 m. sausio 18 d. The New York Times publikacijoje „The secretive company that might end privacy as we know it“ buvo pirmą kartą viešai atskleista „Clearview AI“ veikla. Iki tol bendrovė veikė tyliai ir buvo pranešta, kad jos paslaugomis naudojosi daugiau nei 600 teisėsaugos institucijų, taip pat keletas privačių įmonių.[60] Po šios informacijos paskleidimo įvairiose pasaulio valstybėse kilo susirūpinimas dėl privatumo apsaugos ir teisėtumo šios įmonės veikloje. Jungtinėse Valstijose per

[59] „We are clearview AI“. Clearview Ai , žiūrėta 2025m. balandžio 10d. https://www.clearview.ai/overview
[60] Kashmir Hill, „The Secretive Company That Might End Privacy as We Know It“, žiūrėta 2025m. balandžio 10d.

kelias dienas buvo pateikti aštuoni civiliniai ieškiniai, o vėliau – ir daugiau. Vienas reikšmingiausių – Amerikos pilietinių laisvių sąjungos ieškinys Ilinojuje pagal Biometrinės informacijos privatumo įstatymą (BIPA).[61] Kalifornijoje, 2021 m., pilietinių teisių ir imigrantų teisių gynimo grupės pateikė ieškinį, teigdamos, kad „Clearview“ veikla pažeidžia vietinius draudimus naudoti veido atpažinimo technologijas.

Kanadoje, teisėsaugos institucijos pradėjo tyrimą ir 2021 m. rekomendavo „Clearview“: nutraukti paslaugų teikimą Kanadoje, nutraukti Kanados gyventojų duomenų rinkimą, ištrinti visus šiuos duomenis. Jungtinėje Karalystėje ir Australijoje 2020 m. pradėtas bendras tyrimas dėl asmens duomenų tvarkymo praktikų.[62] Europos Sąjungoje, nors veikla nebuvo tokia aktyvi kaip JAV, buvo vykdomi pavieniai veiksmai. Vokietijoje Hamburgo duomenų apsaugos institucija reikalavo ištrinti konkretaus asmens duomenis, Švedijoje buvo nustatyta, kad policija neteisėtai naudojosi Clearview paslaugomis, pažeisdama Švedijos baudžiamųjų duomenų įstatymą.[63] Tyrimai taip pat buvo pradėti Italijoje.

Galiausiai, Europos duomenų apsaugos valdyba (EDPB) 2020 m. birželio 10 d. pateikė preliminarų vertinimą, kuriame išreiškė rimtų abejonių dėl tokios paslaugos teisėtumo ES teisės kontekste. *„Atsakydama EP nariams dėl „Clearview AI“ priemonės, EDAV taip pat išreiškė savo susirūpinimą dėl tam tikrų veido atpažinimo technologijų pokyčių. EDAV primena, kad pagal Teisėsaugos direktyvą (ES) 2016/680 teisėsaugos institucijos gali tvarkyti biometrinius duomenis siekdamos tik vienareikšmiškai nustatyti fizinio asmens tapatybę ir laikydamosi direktyvos 8 ir 10 straipsniuose nustatytų griežtų sąlygų. EDAV abejoja, ar kuriame nors Sąjungos arba valstybės narėse teisės akte numatytas paslaugos, kurią, pavyzdžiui, suteikia „Clearview AI“ priemonė, naudojimo teisinis pagrindas. Todėl, atsižvelgiant į dabartines aplinkybes ir nedarant poveikio bet kokiam būsimam arba vykdomam tyrimui, tokio naudojimo ES teisėsaugos institucijose teisėtumo negalima įvertinti. Todėl EDAV, nedarydama poveikio tolesnei papildoma informacija grindžiamai analizei, mano, kad tokios paslaugos, kuri, pavyzdžiui, suteikiama taikant priemonę „Clearview AI“, naudojimas Europos Sąjungos teisėsaugos institucijose, atsižvelgiant į dabartines aplinkybes, tikėtina, negalėtų būti suderinamas su ES duomenų apsaugos sistema. Galiausiai EDAV pateikia*

[61] „ACLU sues Clearview AI“. ACLU, žiūrėta 2025m. balandžio 11d. https://www.aclu.org/press-releases/aclu-suesclearview-ai.
[62] „OAIC and UK's ICO open joint investigation into Clearview AI Inc.“. Australijos vyriausybės svetainė, žiūrėta 2025m. balandžio 11d. https://www.oaic.gov.au/news/media-centre/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc.
[63] „IMY (Sweden) - DI-2020-2719 “. GDPR HUB, žiūrėta 2025m. balandžio 11d. https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2020-2719

nuorodas į savo gaires dėl asmens duomenų tvarkymo naudojant vaizdo prietaisus ir praneša apie būsimą darbą dėl veido atpažinimo technologijų naudojimo teisėsaugos institucijose.“[64]

4.1.2 Teisės į privatumą pažeidimai

Tiriant Clearview AI atvejį Europos Sąjungos kontekste ir analizuojant atskirų valstybių narių institucijų veiksmus, paaiškėjo reikšmingi teisės į privatumą ir asmens duomenų apsaugos pažeidimai. Penkios Europos Sąjungos valstybės ir jų duomenų apsaugos institucijos ryškiausiai ėmėsi veiksmų prieš „Clearview AI“.

Jungtinė Karalystė , institucija – Informacijos komisaro biuras (anglų k. Information commissioner‘s office), šios institucijos pagrindinė veikla ginti teises į informaciją visuomenės labui, skatinant viešųjų įstaigų atvirumą ir asmenų duomenų privatumą.[65] Institucija taip pat išskiria dirbtinį intelektą kaip sritį, kuriai skiria prioritetinį dėmesį, nes DI gali kelti didelį pavojų asmenims ir jų teisėms bei laisvėms.[66]

Prancūzija, institucija - Nacionalinė informacinių technologijų ir piliečių laisvių komisija (prancūzų k. Commission Nationale de l'Informatique et des Libertés), tai nepriklausoma Prancūzijos duomenų apsaugos institucija, kuri informuoja gyventojus apie jų teises, nagrinėja skundus ir padeda užtikrinti Bendrojo duomenų apsaugos reglamento laikymąsi. Ji atlieka patikras, taiko sankcijas už privatumo pažeidimus, konsultuoja organizacijas dėl teisėto duomenų tvarkymo bei skatina technologijų, užtikrinančių duomenų apsaugą, plėtrą. [67]

Italija, asmens duomenų apsaugos institucija (italų k. Garante per la protezione dei dati personali), tai nepriklausoma priežiūros institucija, įkurta siekiant apsaugoti asmens duomenų tvarkymą ir užtikrinti žmogaus teisių bei orumo apsaugą tiek viešajame, tiek privačiajame sektoriuose. Institucija veiklą vykdo kaip kolegiali institucija, kurią sudaro keturi parlamento išrinkti nariai, einantys pareigas septynerių metų kadencijai. Ši organizacija siekia užtikrinti, kad visos duomenų

[64] „Europos duomenų apsaugos valdybos (EDAV) trisdešimt pirmoji plenarinė sesija. Darbo grupės dėl mobiliosios programėlės „TikTok“ sudarymas, atsakymas EP nariams dėl „Clearview AI“ priemonės naudojimo teisėsaugos institucijose, atsakymas ENISA patariamajai“. Europos duomenų apsaugos valdyba , žiūrėta 2025m. balandžio 11d. https://www.edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_lt

[65] „Information Commissioner's Office“. Jungtinės Karalystės vyriausybės svetainė, žiūrėta 2025m. balandžio 11d. https://www.gov.uk/government/organisations/information-commissioner-s-office

[66] „Our work on Artificial Intelligence“. ICO , žiūrėta 2025m. balandžio 11d. https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/

[67] „The CNIL‘s missions“. CNIL , žiūrėta 2025m. balandžio 11d. https://www.cnil.fr/en/cnil/cnils-missions

tvarkymo veiklos būtų atliekamos teisėtai ir sąžiningai, o kiekvieno asmens teisės – gerbiamos ir apsaugotos.[68]

Graikija, institucija – Graikijos duomenų apsaugos institucija (anglų k. Hellenic data protection authority). Atsakinga už Bendrojo duomenų apsaugos reglamento taip pat nacionalinių teisės aktų ir įstatymų įgyvendinimo priežiūrą. Veikla apima asmens duomenų apsaugą tiek bendrojo pobūdžio tvarkymo, tiek teisėsaugos tikslais, įskaitant nusikalstamų veikų prevenciją ir tyrimą. Institucija taip pat užtikrina, kad asmenų teisės būtų apsaugotos skaitmeninėje erdvėje, ypač elektroninių ryšių sektoriuje.[69]

Austrija, institucija – Austrijos duomenų apsaugos institucija (austrų k. Datenschutzbehörde). Nacionalinė priežiūros institucija, atsakinga už asmens duomenų apsaugos reglamentų įgyvendinimo priežiūrą Austrijoje. Jos pagrindinė būstinė įsikūrusi Vienoje. Institucija prižiūri asmens duomenų tvarkymą, nagrinėja skundus dėl galimų pažeidimų ir užtikrina, kad būtų laikomasi nacionalinių bei Europos Sąjungos duomenų apsaugos teisės aktų.[70]

Tiriant išvardintų valstybių institucijų atliktus veiksmus prieš „Clearview AI“ įmonę išskiriami šie teisės normų privatumo kontekste pažeidimai:

1) Netinkamas asmens duomenų rinkimas be sutikim. Clearview AI masiškai rinko veido atvaizdus iš viešai prieinamų interneto šaltinių – socialinių tinklų, naujienų portalų, paieškomų asmenų svetainių ir pan. – be asmenų sutikimo ar informavimo. Šie veiksmai pažeidė BDAR 6 straipsnį, nustatantį duomenų tvarkymo teisėtumo pagrindus - *Duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų, ir tik tokiu mastu, kokiu ji yra taikoma:*

a) duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais;

b) tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;

c) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė;

d) tvarkyti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus;

e) tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas;

[68] „The Italian data protection authority: who we are“. GPDP, žiūrėta 2025m. balandžio 11d. https://www.garanteprivacy.it/web/garante-privacy-en/the-italian-data-protection-authority-who-we-are
[69] „Mission“ HDPA , žiūrėta 2025m. balandžio 11d. https://www.dpa.gr/en/hdpa/mission
[70] „Austrian data protection authority“. DSB, žiūrėta 2025m. balandžio 11d. https://data-protection-authority.gv.at/#0

f) tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni, ypač kai duomenų subjektas yra vaikas.[71]

Taip pat 5 straipsnio 1 dalies a punktą, numatantį teisėtumo, sąžiningumo ir skaidrumo principą – *5 straipsnis Su asmens duomenų tvarkymu susiję principai. 1. Asmens duomenys turi būti: a) duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu (teisėtumo, sąžiningumo ir skaidrumo principas);*[72]

2) Biometrinių duomenų tvarkymas be teisinio pagrindo. Veido atvaizdas laikomas biometriniu duomeniu, kuris, pagal BDAR 9 straipsnį, yra laikomas specialios kategorijos asmens duomenimis. *Draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.*[73] Tokie duomenys gali būti tvarkomi tik išimtiniais atvejais – turint aiškų sutikimą arba teisės aktų numatytą pagrindą. „Clearview AI“ neturėjo nei vieno iš šių pagrindų, todėl jų veikla buvo įvardyta kaip neteisėtas jautrių duomenų tvarkymas.

3) Duomenų subjektų teisių pažeidimas. Europos duomenų subjektai neturėjo galimybės pasinaudoti savo teisėmis, kurias garantuoja BDAR 15–18 straipsniai. Asmenys negalėjo: susipažinti su jų duomenimis (15 str.), *Duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir toliau nurodyta informacija....*[74], reikalauti duomenų ištrynimo („teisė būti pamirštam“, 17 str.), *Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis, jei tai galima pagrįsti viena iš šių priežasčių...*[75] apriboti duomenų tvarkymo (18 str.). *Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas apribotų duomenų tvarkymą kai taikomas vienas iš šių atvejų:*

a) asmens duomenų subjektas užginčija duomenų tikslumą tokiam laikotarpiui, per kurį duomenų valdytojas gali patikrinti asmens duomenų tikslumą;

---

[71] Bendrasis duomenų apsaugos reglamentas, žiūrėta 2025m. balandžio 11d.
[72] Ibid
[73] Ibid
[74] Ibid
[75] Ibid

b) asmens duomenų tvarkymas yra neteisėtas ir duomenų subjektas nesutinka, kad duomenys būtų ištrinti, ir vietoj to prašo apriboti jų naudojimą;

c) duomenų valdytojui nebereikia asmens duomenų, duomenų tvarkymo tikslais, tačiau jų reikia duomenų subjektui siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus; arba

d) duomenų subjektas pagal 21 straipsnio 1 dalį paprieštaravo duomenų tvarkymui, kol bus patikrinta, ar duomenų valdytojo teisėtos priežastys yra viršesnės už duomenų subjekto priežastis.[76]

4) Skaidrumo ir informavimo stoka. Clearview AI veikla iki 2020 m. buvo sąmoningai slepiama nuo visuomenės. Nors BDAR 13 straipsnis *Informacija, kuri turi būti pateikta, kai asmens duomenys renkami iš duomenų subjekto* ir 14 straipsnis *Informacija, kuri turi būti pateikta, kai asmens duomenys yra gauti ne iš duomenų subjekto*[77], aiškiai įtvirtina duomenų tvarkymo skaidrumo ir informavimo pareigas, įmonė jų nesilaikė, o tai reiškia esminį skaidrumo principo pažeidimą.

5) Asmens duomenų perdavimas į trečiąsias šalis be tinkamo pagrindo. Kadangi Clearview AI yra registruota JAV, jų veikla apėmė duomenų perdavimą už Europos Sąjungos ribų, nesilaikant BDAR straipsnių:

44 str. Bendras duomenų perdavimo principas;

45 str. Duomenų perdavimas remiantis sprendimu dėl tinkamumo;

46 str. Duomenų perdavimas taikant tinkamas apsaugos priemones;

47 str. Įmonei privalomos taisyklės;

48 str. Sąjungos teisėje neleidžiamas duomenų perdavimas ar atskleidimas;

49 str. Nukrypti leidžiančios nuostatos konkrečiais atvejais;[78]

‚nustatytų duomenų perdavimo į trečiąsias valstybes sąlygų. Nebuvo nei tinkamumo sprendimo, nei sutarčių su apsaugos užtikrinimo priemonėmis, todėl toks perdavimas laikytinas neteisėtu.

4.1.2 Institucijų reakcijos ir sprendimai Europoje ir Europos Sąjungoje

Jungtinės Karalystės informacijos komisaro biuras „ClearView AI“ kompanijai įteikė dvi nacionalines priemones – vykdomąjį pranešimą (anglų k. enforcement notice) ir pranešimą apie piniginę baudą (anglų k. monetary penalty notice.) Vykdomasis pranešimas tai dokumentas, kuriuo reikalaujama sustabdyti ar nutraukti neteisėtą veiklą. Šio pranešimo įteikimą informacijos komisaro

[76] Ibid
[77] Ibid
[78] Ibid

biuras pagrindė teikdami, kad „Clearview AI“ laikoma asmens duomenų valdytoju pagal BDAR ir bendrovės veikla pažeidė Jungtinėje Karalystėje gyvenančių asmenų privatumo teises. Informacijos komisaro biuras nustatė, kad Jungtinių Amerikos Valstijų įmonė rinko ir tvarkė Jungtinės Karalystės biometrinius duomenis, veido atvaizdus, naudodama automatines sistemas pažeidžiant BDAR straipsnius.[79] Dėl šių pažeidimų įteikiant pranešimą dėl piniginės baudos biuras skyrė 7,552,800 GPB (Septynių milijonų penkių šimtų penkiasdešimt dviejų tūkstančių aštuonių šimtų svarų 00 ct) baudą ir nurodė sustabdyti duomenų tvarkymą ir ištrinti surinktus duomenis apie Jungtinės Karalystės gyventojus.[80] „Clearview AI“ bendrovė šiuos veiksmus apskundė pirmojo lygmens tribunolui (anglų k. First-tier tribunal) ir buvo priimtas sprendimas panaikinti baudos skyrimą argumentuojant, kad įmonės veikla nepatenka į BDAR taikymo sritį, kadangi ši veikla buvo vykdoma užsienio teisėsaugos institucijų naudai.[81] Informacijos komisaro biuro pozicija išlieka tvirta, laikomasi pozicijos, kad jei paslaugos teikiamos užsienio teisėsaugos institucijoms, tai nereiškia, kad tokiam duomenų tvarkymui negalioja nacionaliniai duomenų apsaugos reikalavimai, todėl pagal naujausią 2025 metų sausio 31d. pateiktą informaciją, sprendimas buvo apskųstas ir aukštesnysis tribunolas (anglų k. upper tribunal) apeliacinį skundą priėmė. [82]

Prancūzijos duomenų apsaugos institucija, gavus skundus dėl „Clearview AI“ veiklos bendradarbiaujant su kitų ES šalių institucijomis, remiantis gautais skundais atliko tyrimą ir nustatė, kad bendrovė masiškai rinko veido atvaizdus iš viešai prieinamų interneto šaltinių, pavyzdžiui, socialinių tinklų, naujienų portalų. Institucija nustatė esminius BDAR pažeidimus, įskaitant neteisėta duomenų rinkimą be teisinio pagrindo, duomenų subjekto profiliavimą be sutikimo, negalėjimą naudotis prieigos ir ištrynimo teisėmis ir nesklandų bendradarbiavimą su priežiūros institucijomis. „Clearview AI“ įmonė ignoravo Prancūzijos duomenų apsaugos instituciją, tokiu būdų neparodydama noro bendradarbiauti, todėl buvo priimtas sprendimas skirti maksimalią administracinę baudą 20,000,000 eurų (dvidešimt milijonų euru 00ct) baudą bei įpareigojimas nutraukti duomenų rinkimą ir tvarkymą, ištrinti jau surinktus duomenis. [83] Šį sprendimą įmonė turėjo įvykdyti per 2 mėnesių

[79] „Enforcement notice“ ICO, žiūrėta 2025m. balandžio 14d. https://ico.org.uk/media/action-weve-taken/enforcement-notices/4020437/clearview-ai-inc-en-20220518.pdf
[80] „Monetary penalty notice“ ICO, žiūrėta 2025m. balandžio 14d. https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf
[81] First-tier Tribunal bylos nr. EA/20222/0165/FP, žiūrėta 2025m. balandžio 14d. https://www.bailii.org/uk/cases/UKFTT/GRC/2023/819.pdf
[82] „Information Commissioner seeks permission to appeal Clearview AI Inc ruling“. ICO, žiūrėta 2025m. balandžio 14d. https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/
[83] „Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI“. CNIL, žiūrėta 2025m. balandžio 14d.

laikotarpį, tačiau sprendimas nebuvo įvykdytas, todėl 2023 m. balandžio 13 d. papildomai skirtas 5,200,000 eur (penkų milijonų dviejų šimtų tūkstančių eurų 00ct) delspinigių mokėjimas.[84]

Be Jungtinės Karalystės ir Prancūzijos, reikšmingų veiksmų prieš „Clearview AI“ ėmėsi ir kitos Europos Sąjungos valstybės narės – Italija, Graikija ir Austrija. Šių valstybių duomenų apsaugos institucijos, reaguodamos į „Clearview AI“ vykdytą neteisėtą biometrinių duomenų rinkimą be sutikimo ir informavimo, taip pat atliko tyrimus ir skyrė griežtas sankcijas. Tiek Italijos asmens duomenų apsaugos institucija[85], tiek Graikijos duomenų apsaugos institucija[86] nustatę reikšmingus BDAR pažeidimus, skyrė maksimalaus dydžio baudas – po 20 mln. eurų. Austrijos duomenų apsaugos institucija savo ruožtu taip pat pripažino „Clearview AI“ veiklą neteisėta, nors tuo metu finansinė sankcija nebuvo taikyta, tačiau neatmetė galimybės ją skirti ateityje.[87]

Tokie Europos Sąjungos valstybių institucijų atlikti tyrimai ir jų priimti sprendimai atskleidžia bendrą visų institucijų poziciją, kad BDAR nuostatos taikomos, kai duomenys tvarkomi apie Europos Sąjungos teritorijoje esančius asmenis, neatsižvelgiant į tai, kad bendrovė yra įsikūrusi Jungtinėse Amerikos Valstijose. Šis atvejis parodė ne tik praktinį asmens duomenų apsaugos normų taikymą, bet ir iškėlė klausimus dėl dirbtinio intelekto poveikio asmens privatumui.

4.1.3 Reikšmė teisės į privatumą kontekste

Išanalizavus šio atvejo faktines aplinkybes, teisės į privatumą pažeidimus bei Europos Sąjungos narių institucijų veiksmus prieš „Clearview AI“ įmonę, pastebėtina, kad pirmiausia šis atvejis formuoja vieningą asmens duomenų apsaugos institucijų poziciją, kuria nurodoma, kad net jei įmonė savo technologijų veiklą realizuoja už Europos Sąąjungos ribų, ji privalo laikytis bendrų Europos Sąjungos teisės aktų, tokių kaip BDAR, jei ši tvarko ES piliečių duomenis. Šis atvejis išryškino ir kitus svarbius aspektus teisės į privatumą kontekste, pavyzdžiui, kad biometrinių duomenų

https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf

[84] „Facial recognition: the French SA imposes a penalty payment on CLEARVIEW AI“. EDPB, žiūrėta 2025m. balandžio 14d. https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

[85] „Facial recognition: Italian SA fines Clearview AI EUR 20 million“. EDPB, žiūrėta 2025m. balandžio 14d. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

[86] „Hellenic DPA fines Clearview AI 20 million euros”. EDPB, žiūrėta 2025m. balandžio 14d. https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

[87] „Decision by the Austrian SA against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR“ . EDPB, žiūrėta 2025m. balandžio 14d. https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en

apsauga, asmens atvaizdo apsauga yra išskiriamos kaip ypač jautrios sritys, todėl esant grėsmėms šiems duomenims institucijos nedelsiant imasi veiksmų ir skiria ypač griežtas sankcijas už nustatytus pažeidimus ir tokios grėsmes Europos Sąjungoje nėra ignoruojamos.

Šis atvejis taip pat pabrėžia technologijų plėtros suderinamumą kartu su žmogaus teisėmis svarbumą, tai rodo signalą technologijų įmonėms, kad nesvarbu kokį pažangumą ir kokias galimybes gali rodyti dirbtinis intelektas, kuriant ir naudojant sistemas jas būtina derinti su galiojančiais įstatymais ir kad už jų ignoravimą galima susilaukti ypač didelių nuobaudų. Technologijų plėtra privalo būti suderinta su žmogaus teisėmis.

4.1.4 „Clearview AI“ atvejo vertinimas pagal Europos Sąjungos DI aktą

Atkreiptinas dėmesys, kad šis atvejis institucijų buvo vertinamas remiantis BDAR normomis, kadangi tuo metu Europos Sąjungos dirbtinio intelekto aktas dar nebuvo įsigaliojęs, todėl šiuo tyrimu taip pat buvo siekiama įvertinti kaip šiuo atveju „ClearView AI“ įmonės veikla būtų vertinama remiantis naujai įsigaliojusio Europos Sąjungos dirbtinio intelekto akto nuostatomis, kaip būtų vertinama šios įmonės veikla, kokie būtų skirtumai taikant DI aktą lyginant su BDAR.

Remiantis dirbtinio intelekto aktu, manytina, kad „Clearview AI“ pažeidė bent vieną aiškiai įtvirtintą draudimą. Tam tikros DI sistemos yra visiškai draudžiamos, jei kelia nepriimtiną riziką. Pavyzdžiui – ES DI akto 5 straipsnio e skirsnis, „pateikti rinkai, pradėti naudoti šiuo konkrečiu tikslu arba naudoti DI sistemas, kuriomis kuriamos arba išplečiamos veido atpažinimo duomenų bazės, netikslingai renkant veido atvaizdus iš interneto arba apsauginių vaizdo stebėjimo sistemų (AVSS) įrašų“

„Clearview AI“ savo sistemai automatizuotai rinko veido atvaizdus iš viešai prieinamų internetinių šaltinių, įskaitant socialinius tinklus, naujienų portalus, viešus vaizdo įrašus. Tokiu būdų šie atvaizdai buvo naudojami sukurti biometrinių duomenų bazei, kuri vėliau buvo komerciniais pagrindais siūloma teisėsaugos institucijoms. Manytina, kad tokia praktika tiesiogiai atitinka draudžiamą veiklą pagal cituota DI akto 5 straipsnį, nes duomenys buvo renkami netikslingai, be sutikimo iš viešos interneto erdvės. Dirbtinio intelekto akto 1 straipsnyje nustatytą reglamento taikymo sritį, akivaizdu, kad „Clearview AI“ įmonės veikla būtų patekusi į reglamento taikymo ribas. Pagal DI akto 1 straipsnio a,c, dalis DI aktas taikomas tiek tiekėjams, tiek diegėjams, nepriklausomai nuo to, ar jie yra įsisteigę Europos Sąjungoje, ar trečiojoje valstybėje, jeigu jų DI sistemos yra naudojamos Sąjungoje arba daro poveikį Sąjungos gyventojams. Nors Clearview AI yra įsikūrusi

Jungtinėse Amerikos Valstijose, ši bendrovė rinko ir tvarkė Europos Sąjungos šalių piliečių biometrinius duomenis, veido atvaizdus ir siūlė savo technologiją naudoti teisėsaugos institucijoms keliose ES valstybėse narėse, įskaitant Švediją, Italiją, Prancūziją bei Austriją. Tokie veiksmai aiškiai atitinka DI akto nuostatas.

Atsižvelgiant į tai, kad praktikoje institucijos taikė griežčiausias bausmes remiantis BDAR nuostatomis, ir į tai, kad remiantis DI aktu šios bendrovės technologija būtų įtraukiama į draudžiamų naudoti sistemų sritį, manytina, kad tokioje situacijoje taikant DI aktą taip pat būtų skiriamos griežtos bausmės, numatytos akto 99 straipsnyje – „Už 5 straipsnyje nurodytų su DI susijusios praktikos draudimų nesilaikymą skiriamos iki 35 000 000 EUR dydžio administracinės baudos arba, jei pažeidėjas yra įmonė, iki 7 % jos bendros pasaulinės praėjusių finansinių metų metinės apyvartos, atsižvelgiant į tai, kuri yra didesnė.“

„Clearview AI“ atvejis atskleidė grėsmes, kurias gali kelti dirbtinio intelekto pagrindu veikiančios biometrinių duomenų sistemos asmens teisėms į privatumą. Įmonės vykdyta neteisėta veido atvaizdų rinkimo praktika, duomenų subjektų teisių ignoravimas, duomenų perdavimas į trečiąsias šalis be apsaugos priemonių ir sutarčių – visa tai parodė, kaip modernios technologijos gali būti naudojamos pažeidžiant žmogaus teisių principus. Europos Sąjungos valstybės narės, pasitelkusios savo duomenų apsaugos institucijas, reagavo vieningai – taikė dideles finansines sankcijas ir priėmė sprendimus dėl duomenų pašalinimo bei veiklos nutraukimo. Analizuojant šį atvejį pagal Europos Sąjungos dirbtinio intelekto aktą, aiškiai matyti, kad tokia sistema patenka į draudžiamų naudoti DI sistemų kategoriją, todėl sankcijos galėtų būti dar griežtesnės nei pagal BDAR.

Šis atvejis tampa reikšmingu ne tik teisės praktikoje, bet ir kuriant aiškesnius dirbtinio intelekto reguliavimo standartus, siekiant išvengti piktnaudžiavimo asmens duomenimis ateityje. Toliau darbe analizuojamas kitas garsus atvejis įmonės „Cambridge Analytica“, kuris, nors ir paremtas skirtinga technologija, taip pat susijęs su duomenų naudojimu be aiškaus sutikimo ir atskleidžia kitokį dirbtinio intelekto įrankių panaudojimo būdą – manipuliuoti gautais asmens duomenimis siekiant padaryti įtaką jų politiniams pasirinkimams.

4.2 „Cambrigde Analytica“ atvejo analizė

Įmonė „Cambridge Analytica“, įkurta Jungtinėje Karalystėje, save pristatė kaip pažangią duomenų analizės bendrovę, kuri padeda pasiekti tam tikras grupes asmenų remiantis jų elgesiu,

nuomonėmis ir įpročiais. Jie teigė, kad naudoja daugybę informacijos apie žmonių amžių, pomėgius, politines pažiūras ir net psichologinius bruožus tam, kad galėtų sukurti labai tikslias rinkodaros žinutes. Įmonė taip pat naudojo sudėtingus duomenų analizės ir prognozavimo metodus, kad atpažintų žmonių grupes, kurios elgiasi panašiai, ir joms pateiktų specialiai pritaikytą turinį. Ši informacija buvo renkami iš skirtingų šaltinių, kartais net be žmonių sutikimo, o jos pagrindu buvo daromi sprendimai politinėse kampanijose ir reklamoje.[88] Paprastai paaiškinant, ši sistema veikė taip: jei asmuo socialiniuose tinkluose spaudė „patinka“ tam tikriems įrašams, žiūrėjo konkretaus tipo vaizdo įrašus, naršė tam tikrus puslapius ar dalijosi tam tikru turiniu – visa ši veikla buvo analizuojama, siekiant sudaryti psichologinį žmogaus portretą. Remiantis šiuo portretu, asmeniui naršant internete buvo pritaikytos politinės žinutės ar reklama, kuri turėjo paveikti jo nuomonę ar elgesį.

Apibendrinant galima išskirti svarbiausius šios įmonės veiklos bruožus: tai buvo privati duomenų analizės įmonė, ji padėjo politinėms partijoms ir verslams pasiekti tikslines žmonių grupes, duomenys buvo renkami iš įvairių viešų ir ne visada skaidrių šaltinių, taikytas žmonių vertinimas, jų asmenybės, vertybių ir elgsenos analizė, sukurtas turinys buvo pritaikomas konkrečioms grupėms ir joms rodomas per įvairius skaitmeninius, socialinius kanalus.

4.2.1 CA Atvejo Faktinės aplinkybės

2014 m. psichologas Aleksandras Koganas, dirbęs Kembridžo universitete, sukūrė asmenybės testo aplikaciją „this is your digital life“, kuri rinko duomenis ne tik iš naudotojų, kurie patys atsakė į klausimus, bet ir iš jų „Facebook“ draugų.[89] Ši aplikacija buvo pristatoma kaip asmenybės testai, pagrįsti psichologiniu „Didžiojo penketo“ (anglų k. OCEAN) modeliu, kuris vertina penkias asmenybės savybes: ar asmenims patinka naujos patirtys, ar asmenys mėgsta planus ir tvarką, ar asmenims patinka leisti laiką su kitais žmonėmis, ar jie noriai leidžia laiką su kitais žmonėmis, ar jie kitų poreikius iškelia aukščiau savo bei ar asmenys dažnai linkę nerimauti. Manytina, kad programėlė buvo naudojama kaip priedanga, pristatant ją kaip skirtą moksliniams tyrimams psichologijos mokslo kontekste. Vartotojai, norėdami dalyvauti teste, turėjo prisijungti prie aplikacijos naudodami savo „Facebook“ paskyrą. Dėl tuo metu galiojančių vidinių socialinio tinklo nuostatų, kurios suteikė galimybę aplikacijoms naudotis „Facebook API“ (anglų k. application

[88] „Cambridge Analytica“ Web Archive tinklalapio archyvas, žiūrėta 2025m. balandžio 16d. https://web.archive.org/web/20160216023554/https://cambridgeanalytica.org/services

[89] Ikhlaq ur Rehman „Facebook-Cambridge Analytica data harvesting: What you need to know“. *Library Philosophy and Practice* (2019), žiūrėta 2025m. balandžio 16d. https://core.ac.uk/download/pdf/220153793.pdf

programming interface), aplikacijai buvo leidžiama prieiga prie daugybės duomenų, pavyzdžiui, vardai, pavardės, nuotraukos, el. paštas, mėgstamas turinys, ką asmeniui patinka skaityti, kokie jam puslapiai patinka. Aplikacija galėjo rinkti duomenis ne tik apie asmenį, kuris naudojo ją, bet ir apie to asmens draugus, neatsižvelgiant į tai, kad jie nenaudojo aplikacijos. Tokiu būdu buvo surinkti duomenys apie maždaug 87 milijonus vartotojų, nors iš jų aplikaciją tiesiogiai naudojo tik apie 270 000.

Surinkti duomenys buvo perduoti „Cambridge Analytica“, kuri juos naudojo psichologinių profilių kūrimui bei politinių reklamų taikymui pagal naudotojų asmenybės bruožus. Tokiu būdu įmonė siekė paveikti rinkėjų nuomonę rinkimų metu. Vienas iš pavyzdžių, kaip šie duomenys buvo pritaikyti praktikoje, buvo 2016 m. JAV prezidento rinkimai, kuriuose „Cambridge Analytica“ prisidėjo prie Donaldo Trumpo kampanijos. Įmonė buvo kaltinama tuo, kad pasitelkdama surinktus duomenis paveikė rinkėjų sprendimus. Ypatingą dėmesį sukėlė naudojama strategija, vadinama „tamsieji įrašai“ (anglų k. dark posts) – tai individualios reklamos, kurios buvo matomos tik konkrečiai tiems asmenims, kuriems šios reklamos buvo taikomos.[90]

Pažymėtina, kad šis atvejis turėjo įtakos ne tik JAV politinei sistemai, bet ir Europos Sąjungos kontekste. Nors Jungtinė Karalystė 2020 m. sausio 31 d. oficialiai pasitraukė iš Europos Sąjungos, „Cambridge Analytica“ duomenų rinkimas ir panaudojimas vyko tuo laikotarpiu, kai šalis dar buvo ES narė, todėl šio atvejo analizė ir vertinimas pagrįstai priskirtinas ES duomenų apsaugos kontekstui. Taip pat Jungtinės Karalystės duomenų apsaugos institucija įtarė CA įmonę dėl teisės pažeidimų ir atliko tyrimą, kuris toliau bus nagrinėjamas kitame poskyryje.

4.2.2 Institucijų reakcijos ir teisės pažeidimai

Analizuojant šį atvejį nustatyta, kad vienintelės valstybės, tuo metu buvusios Europos Sąjungos nare, Jungtinės Karalystės duomenų apsaugos institucija reagavo į „Cambrigde Analytica“ įmonės veiklą. Manytina, kad tokį rezultatą lėmė aplinkybės tokios kaip CA įmonė buvo įsikūrusi JK ir vykdė savo veiklą iš ten esančios būstinės, bei politinė situacija, tuo metu vyraujanti Jungtinėje Karalystėje dėl „Brexit“ referendumo. Jungtinės Karalystės informacijos komisaro tarnyba oficialų tyrimą dėl asmens duomenų naudojimo politinėje reklamoje pradėjo 2017 m. gegužės mėnesį, reaguodama į tarptautinės žiniasklaidos pranešimus apie galimą „Cambridge Analytica“ (CA)

[90] Ibid

bendrovės neteisėtą vartotojų duomenų išnaudojimą. Tai buvo vienas iš didžiausiu tokio pobūdžio tyrimu duomenų apsaugos institucijos istorijoje. Tyrimo metu ICO analizavo daugiau nei 700 terabaitų duomenų, išdavė 31 informacinį pranešimą, surengė kratas ir nustatė 71-ą su byla susijusi liudytoją.

Pagrindinis dėmesys buvo sutelktas į tai, kaip CA, per Dr. Aleksandro Kogano sukurtą programėlę „This is your digital life“, pasinaudojusi „Facebook“ API, surinko apie 87 milijonų vartotojų – tiek pačių dalyvavusių apklausoje, tiek jų draugų – duomenis. Institucija nustatė, kad CA pažeidė pirmąjį tuo metu iki BDAR įsigaliojimo buvusio nacionalinio duomenų apsaugos įstatymo 1998 m. principą – dėl nesąžiningo asmens duomenų tvarkymo politiniais tikslais , t. y. asmens duomenys buvo renkami nesąžiningai, nepakankamai informuojant duomenų subjektus, ir buvo naudojami nesant teisėto pagrindo, ypač politinio profiliavimo tikslais. Tyrime taip pat buvo nagrinėtas CA ryšys su „Leave.EU“ – viena iš „Brexit“ kampanijos organizacijų. Nors žiniasklaidoje ir viešuose pasisakymuose buvo teigiama apie jų bendradarbiavimą, tyrimas parodė, kad tarp šių šalių įvyko tik keturi susitikimai, tačiau joks oficialus bendradarbiavimas nebuvo užmegztas.

Jungtinės Karalystės informacijos komisaro biuras savo galutinėje 2018 m. ataskaitoje nurodė, kad įmonė „Cambridge Analytica“: pažeidė tuo metu galiojantį nacionalinį asmens duomenų apsaugos įstatymą, nesuteikė asmenims tinkamos informacijos apie jų duomenų naudojimą, neturėjo aiškaus teisinio pagrindo duomenų rinkimui iš draugų profilių, naudojant aplikaciją, ir neužtikrino pakankamo skaidrumo dėl savo veiklos.[91]

Jungtinėje Karalystėje galiojant 1998 duomenų apsaugos įstatymui, baudos buvo labai ribotos iki 500,000 GBP. Iki įsigaliojant BDAR , duomenų apsaugos institucija neturėjo įgaliojimų skirti milijoninių baudų. Informacijos komisaro biuras planavo skirti baudą, bet tyrimui pasiekus kulminaciją, įmonė „Cambrigde Analytica“ buvo paskelbusi bankrotą, todėl nė viena bausmė skirta tiesiogiai „Cambridge Analytica“ nebuvo skirta ir įvykdyta. Šio atvejo kontekste tyrimo metu buvo skirta 500,000 GPB baudą kompanijai „Facebook“ už tai, kad leido šiai veiklai vykti dėl netinkamų vidinių taisyklių, kurios neapsaugojo asmens duomenų.

Reaguodamas į šias aplinkybes ir vis didėjantį viešą susirūpinimą, Europos Parlamentas 2018 m. spalio 25 d. priėmė rezoliuciją, kurioje įvardijo „Cambridge Analytica“ atvejį kaip reikšmingą demokratinių procesų pažeidimo pavyzdį. Joje pažymėta, kad bendrovė neteisėtai rinko ir analizavo duomenis be naudotojų sutikimo, o tokie veiksmai kelia grėsmę rinkimų sąžiningumui. Parlamento

[91] „Investigation into the use of data analytics in political campaigns“. ICO, žiūrėta 2025m. balandžio 18d. https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

nuomone, reikalinga griežtesnė ES duomenų apsaugos priežiūra, daugiau skaidrumo rinkimų reklamoje ir tikslesnis algoritmų naudojimo reglamentavimas.[92]

4.2.3 Reikšmė privatumo kontekste

„Cambridge Analytica“ atvejis tapo pavyzdžių, kaip asmens duomenys gali būti panaudojami ne visai skaidriai ir netgi paveikti politinius procesus. Šiuo atveju buvo aiškiai matoma, kad žmonių duomenys buvo renkami ne tik iš jų pačių, bet ir per draugus, naudojantis socialinių tinklų sistemomis. Tokiu būdu daug žmonių nežinojo, kad jų informacija buvo naudojama – ir tam nebuvo duotas joks sutikimas. Tokie atvejai mažina pasitikėjimą skaitmenine erdve ir išryškina, kad grėsmės teisei į privatumą gali likti ir nepastebimos. Ši situacija parodė, kaip mažai žmogus gali turėti kontrolės, kas nutinka su jo duomenimis internete, net jei pats tiesiogiai niekur nedalyvavo. Ypač didelį nerimą kėlė tai, kad surinkta informacija buvo naudojama politiniais tikslais – pagal žmogaus pomėgius buvo rodoma konkreti reklama ar žinutės, kurios galėjo paveikti jo nuomonę.

Visa tai privertė įstatymų kūrėjus ir turinčius kompetencijas duomenų apsaugos srityje iš naujo pagalvoti, kaip svarbu yra skaidriai tvarkyti duomenis ir užtikrinti, kad žmonės tikrai žinotų, kaip jų informacija naudojama. Tai parodė, kad vien techninių galimybių nepakanka – būtina aiški teisė, žmonių informavimas ir atsakomybė. Šis atvejis tapo stipriu signalu, kad reikia geresnės priežiūros ir griežtesnių taisyklių, kad panašios situacijos nepasikartotų. Manytina, kad šis atvejis prisidėjo prie viešo, politinio ir institucijų dėmesio į BDAR svarbą ir padėjo paskatinti jo griežtesnį įgyvendinimą.

4.2.4 „Cambrigde analytica“ atvejo vertinimas pagal Europos Sąjungos DI aktą.

Vertinant CA veiklą pagal DI akto nuostatas, nekyla abejonių, ar jų taikyta duomenų analizės sistema, pagrįsta profiliavimu ir automatizuotu sprendimų priėmimu, nepažeistų DI akte nustatytų ribojimų ar draudimų. Pavyzdžiui, pagal DI akto 5 straipsnio a dalį draudžiama – „naudoti DI sistemą,

[92] “rezoliucija 2018/2855(RSP)”. Europos Parlamentas, žiūrėta 2025m. balandžio 18d. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52018IP0433&

kurioje pasitelkiami pasąmonę veikiantys metodai, kurių asmuo nesuvokia, arba tikslingai pasitelkiami manipuliavimo ar apgaulės metodai, siekiant iš esmės pakeisti asmens ar asmenų grupės elgesį arba tą elgesį iš esmės pakeičiant, pastebimai susilpninant jų gebėjimą priimti pagrįstą sprendimą, taip juos priverčiant priimti sprendimą, kurio jie kitu atveju nebūtų priėmę...“[93] Atsižvelgiant į tai, kad CA naudodavo reklamas, kurios buvo tikslingai rodomos konkretiems žmonėms, remiantis jų psichologiniu profiliu, galima teigti, kad tai galėtų būti vertinama kaip bandymas pasinaudoti žmogaus psichologiniu pažeidžiamumu.

Žvelgiant per Europos Sąjungos dirbtinio intelekto akto 5 straipsnio c dalies prizmę, argumentuotina, kad „Cambridge Analytica“ veikla teoriškai atitiko tam tikrus draudžiamos praktikos požymius. EU DI Akto 5 straipsnio c dalis – „pateikti rinkai, pradėti naudoti arba naudoti DI sistemas fiziniams asmenims ar asmenų grupėms tam tikru laikotarpiu vertinti ar klasifikuoti pagal jų socialinį elgesį arba žinomus, numanomus ar nuspėjamus asmeninius ar asmenybės bruožus, kai socialinis reitingas lemia vieną arba abu toliau išvardytus dalykus: i) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar asmenų grupėmis socialiniuose kontekstuose, kurie nėra susiję su kontekstais, kuriuose duomenys buvo iš pradžių sugeneruoti ar surinkti; ii) žalingą ar nepalankų elgesį su tam tikrais fiziniais asmenimis ar asmenų grupėmis, kuris yra nepagrįstas arba neproporcingas jų socialiniam elgesiui ar jo pavojingumui;“ Aiškinant paprasčiau, manytina, kad šio draudimo esmė apsaugoti žmones nuo to, kad jie nebūtų neteisingai vertinami pagal jų elgesį, ypač kai tas elgesys neturi nieko bendro su situacija, kurioje vėliau tai panaudojama. Pavyzdžiui, jeigu žmogus „Facebook“ spaudžia „patinka“ patriotiškiems įrašams ar straipsniams apie saugumą, tai dar nereiškia, kad jam reikia rodyti vienos partijos politines reklamas ar šališką informaciją apie imigraciją. Arba jeigu žmogus internete domisi sveikata ir alternatyvia medicina, tai jis neturėtų būti automatiškai priskirtas nepasitikinčių mokslu kategorijai ir būti pastoviai gaunančiam dezinformacija. Tai apsaugo žmones nuo klaidingo įspūdžio sudarymo vien remiantis jų paspaudimais ar naršymo įpročiais. „Cambridge Analytica“ rinko ir analizavo socialiniuose tinkluose vartotojų pateikiamus duomenis, sukūrė psichologinius profilius ir juos naudojo politiniams tikslams – siekdama paveikti žmonių nuomonę bei elgseną rinkimuose.

Atsižvelgiant į šias nuostatas, galima manyti, kad jei CA veikla būtų vertinama pagal naująjį DI aktą, būtų pagrįstų prielaidų taikyti 5 straipsnyje nurodytus draudimus. O tai reikštų galimybę skirti atitinkamai griežtas baudas, kaip numatyta DI akto 99 straipsnyje – iki 35 mln. eurų arba 7 % pasaulinės metinės apyvartos, bei įmonės sistemos būtų laikytinos draudžiamų praktikoje grupėje.

[93] Ibid

4.3 Atlikto tyrimo rezultatų apibendrinimas

Analizuojant abu atvejus, autoriui ypač nerimą kėlė tai, kaip giliai tokios sistemos gali įsiskverbti į mūsų kasdienį privatumo lauką, praktiškai be individo žinios ar sutikimo. Tiek „Clearview AI“, tiek „Cambridge Analytica“ atvejai parodė, kad grėsmės asmens teisėi į privatumą kyla ne iš pačios dirbtinio intelekto technologijos, o iš to, kas ir kokiu tikslu šias sistemas kuria ir naudoja. Abi įmonės naudojo DI priemones asmens duomenims rinkti, vertinti, profiliuoti ar atpažinti – be tinkamo teisinio pagrindo, skaidrumo ar duomenų subjektų sutikimo. Tai įrodo, kad subjektai, naudojantys dirbtinio intelekto sistemas neetiškais tikslais, o ne pati technologija, kelia grėsmes ir pažeidžia žmogaus teises.

Abi analizės rodo, kad automatizuotas elgesio vertinimas ir profiliavimas remiantis dirbtiniu intelektu gali būti naudojamas ne tik komerciniais, bet ir manipuliacijos tikslais – ypač politikos ar teisėsaugos srityse. Tokios technologijos kuria nelygias sąlygas ir gali lemti diskriminacinius, neproporcingus veiksmus prieš asmenį, net jei jis nieko aktyviai sąmoningai nedarė – tik įprastai naršė savo socialiniuose tinkluose. Abi įmonės, viena rinkdama biometrinius duomenis, kita socialinių tinklų veiklą, neužtikrino duomenų subjektų informavimo, sutikimo ir kontrolės. Tai rodo, kad skaidrumas technologijų srityje yra itin silpna grandis. Daugelis vartotojų nežino, kokiu mastu jų duomenys naudojami ir kokie sprendimai priimami remiantis tuo.

Tyrimas atskleidė, kad žmonių teisės buvo pažeidžiamos net ir tiems, kurie nieko nepaspaudė ar niekur nedalyvavo, patys nesutiko teikti savo duomenų. Tai reiškia, kad vien žmogaus atsargumo nepakanka, o sistemos turi būti kuriamos taip, kad būtų atsižvelgiama į asmens teisę į jo privatumą iš principo, nepriklausomai nuo jo veiksmų. Nors BDAR suteikia stiprų apsaugos pagrindą, praktikoje ne visos institucijos reagavo vienodai greitai ar griežtai. Kai kur tyrimai buvo pavėluoti, sankcijos simbolinės, arba įmonės tiesiog spėjo bankrutuoti. Tai rodo, kad reguliavimas turi būti ne tik aiškus, bet ir veiksmingas bei laiku taikomas. Abu atvejai parodė, kad BDAR ne visada pakanka įvertinti DI sistemų elgseną. Europos Sąjungos dirbtinio intelekto aktas atneša aiškesnį požiūrį į pavojingas sistemas, jų klasifikavimą, draudimus ir baudų skyrimą. Tyrimas rodo, kad taikant DI aktą šioms situacijoms, sankcijos būtų buvusios dar griežtesnės, o įmonių veikla – aiškiai uždrausta.

TYRIMO IŠVADOS IR PASIŪLYMAI

Šio darbo rengimo metu autoriui tapo akivaizdu, jog technologinė pažanga verčia iš naujo permąstyti ne tik teisines normas, bet ir pačią žmogaus teisės į privatumą sampratą, dar kartą teko susimąstyti, kaip greitai gali keistis visas pasaulis bei kokią milžinišką įtaką mūsų kasdienybei daro sparčiai tobulėjančios technologijos. Nors jos atveria plačias galimybes, jos taip pat kelia rimtų iššūkių žmogaus teisėms, todėl būtina nuolatinė šių procesų priežiūra, stebint, ar taikomi teisiniai instrumentai spėja prisitaikyti ir veiksmingai apsaugoti privatumo ribas šiuolaikinėje skaitmeninėje aplinkoje.

Atsižvelgiant į atliktą tyrimą ir išanalizuotus atvejus, pateikiamos šios pagrindinės darbo išvados, ginamųjų teiginių analizė ir pasiūlymai:

1. Išanalizavus dirbtinio intelekto sampratą, raidą ir pagrindines savybes, galima teigti, kad tai sparčiai besivystanti ir daugiasluoksnė technologija, kurios apibrėžimas priklauso nuo požiūrio – mokslinio, praktinio ar technologinio. DI ištakos siekia dar senovės filosofiją ir mitologiją, o šiandien jis tampa vis labiau neatsiejamas nuo kasdienio gyvenimo. Nors vieningo apibrėžimo nėra, dauguma šaltinių sutaria, kad DI tai gebėjimas automatizuotai atlikti užduotis, reikalaujančias žmogaus intelekto. Jo klasifikacija pagal veikimo principą, intelekto lygį ir taikymo sritį padeda geriau suprasti, kokios technologijos laikomos DI ir kokiose srityse jos naudojamos. Istorinė raida rodo, kaip DI perėjo nuo idėjų prie praktinio taikymo, o šiandieninės galimybės kelia ir naujus klausimus dėl jo poveikio žmogui ir jo teisėms.

2. Išanalizavus asmens teisės į privatumą sampratą ir jos reikšmę DI kontekste, galima teigti, kad ši teisė per ilgą istoriją išsiplėtė nuo fizinės erdvės apsaugos iki skaitmeninio duomenų kontrolės. Šiuolaikinė visuomenė ir DI technologijų plėtra lėmė tai, kad privatumo sąvoka nebėra suprantama tik kaip kūno ar namų neliečiamumas – šiandien ji vis labiau siejama su teise valdyti informaciją apie save skaitmeninėje erdvėje. DI gebėjimas automatizuotai rinkti, analizuoti ir prognozuoti remiantis asmens duomenimis kelia rimtų grėsmių informaciniam savarankiškumui. Todėl apsauga nuo neteisėto duomenų naudojimo tampa esmine privatumo dalimi. Ši teisės transformacija rodo, kad DI eroje privatumas turi būti suvokiamas kaip teisė į duomenų kontrolę, o ne tik kaip fizinės erdvės neliečiamumas.

3. Dabartinis asmens teisės į privatumą teisinis reglamentavimas Lietuvos Respublikoje dirbtinio intelekto kontekste visų pirma grindžiamas Europos Sąjungos taikomu Bendruoju duomenų apsaugos reglamentu, kuris užtikrina pagrindinius duomenų apsaugos principus ir tiesiogiai taikomas valstybėse narėse. Naujausias ir reikšmingiausias žingsnis šioje srityje, dirbtinio intelekto akto

priėmimas, kuris tampa pirmuoju pasaulyje teisės aktu, sistemingai reglamentuojančiu DI naudojimą bei siekiančiu užtikrinti žmogaus teises, įskaitant ir teisę į privatumą, technologijų plėtros fone. Nacionalinių teisės aktų, tiesiogiai reglamentuojančių DI ir privatumo sąveiką, šiuo metu Lietuvoje nėra, manytina, kad gali būti taikomis bendrosios Konstitucijos, Baudžiamojo ir Darbo kodeksų nuostatos, kurios, darbo autoriaus nuomone, teoriškai gali būti pritaikomos šioje srityje. Vis dėlto, tiek Lietuva, tiek visos ES valstybės narės aktyviai rengiasi dirbtinio intelekto akto įgyvendinimui, plėtoja nacionalines priemones ir formuoja atsakingų institucijų tinklą, siekdamos užtikrinti praktinį šio teisės akto taikymą.

4. Dirbtinio intelekto technologijų taikymo praktinis poveikis asmens teisės į privatumą apsaugai, analizuojant „Clearview AI“ ir „Cambridge Analytica“ atvejus, atskleidžia, kad pagrindinės grėsmės kyla ne iš pačios technologijos, bet iš to, kaip ir kokiais tikslais ji yra naudojama. Abi nagrinėtos bylos parodė sistemingus privatumo pažeidimus – nuo biometrinių duomenų neteisėto rinkimo be sutikimo iki asmens psichologinio profilio sudarymo ir naudojimo manipuliacijos politiniais tikslais. Tyrimas įrodė, kad esamas duomenų apsaugos instrumentas - bendrasis duomenų apsaugos reglamentas suteikia teisinį pagrindą reaguoti į tokius pažeidimus, tačiau praktikoje šio instrumento normų taikymas ne visada buvo pakankamai greitas ar efektyvus, ypač kai veikla vykdyta iš užsienio arba kai įmonės siekė išvengti atsakomybės. Europos Sąjungos Dirbtinio intelekto aktas teoriškai būtų leidęs tokias praktikas įvardyti kaip draudžiamas – tiek dėl netikslingo biometrinių duomenų rinkimo, tiek dėl profiliavimo metodų. Tai rodo, kad naujasis reguliavimas turi didelį potencialą efektyviau apsaugoti asmens teisę į privatumą DI kontekste, aiškiai identifikuojant rizikingas ar neteisėtas sistemas. Tuo pačiu, tyrimas atskleidė svarbią įžvalgą: vien techninės pažangos nepakanka, būtinas skaidrumo, informavimo ir asmens kontrolės duomenų atžvilgiu stiprinimas. Šie atvejai ne tik atskleidė realias rizikas, bet ir padėjo formuoti stipresnį visuomenės bei politinį spaudimą tobulinti asmens duomenų apsaugos sistemą tiek ES, tiek pasauliniu mastu.

Ginamųjų teiginių analizė:

1. Pirmasis ginamasis teiginys, kad dirbtinio intelekto technologija savaime nėra grėsmė asmens teisei į privatumą, pasitvirtino. Atliekant tyrimą įrodyta, kad pagrindinės grėsmės kyla dėl žmogaus veiksmų, sistemų kūrėjų ir naudotojų sprendimų, kurie lemia, kokiu tikslu bus naudojamos DI sistemos.

2. Antrasis ginamasis teiginys taip pat pasitvirtino. Įrodyta, kad vien teisės aktų neužtenka – vartotojų sąmoningumas ir kūrėjų atsakomybė yra esminės privatumo apsaugos sąlygos. Nors asmens

duomenys saugomi įstatymų, geriausiai savo duomenis gali apsaugoti pats asmuo, įvertindamas aplinkos, kurioje nori pateikti savo duomenis, saugumą ir patikimumą.

3. Trečiasis ginamasis teiginys pasitvirtino iš esmės. ES Dirbtinio intelekto aktas įvertintas kaip pirmasis sisteminis tokio pobūdžio teisės aktas pasaulyje, kurio struktūra, rizikų vertinimas ir draudimų mechanizmas gali būti perimtas ir kitų valstybių teisėkūroje. Patvirtinti teiginį, ar šis aktas taps pavyzdžiu visam pasauliui, reikia laiko ir praktikos taikant šį aktą.

Dirbtinio intelekto technologijos atveria plačias galimybes inovacijoms, tuo pačiu kelia reikšmingų iššūkių asmens teisės į privatumą apsaugai. Nagrinėti atvejai atskleidė konkrečius pažeidimus ir institucinės reakcijos spragas, o teisinis reguliavimas, nors ir stiprus ES lygmeniu, ne visada buvo pakankamai greitai ar aiškiai taikomas praktikoje. Atsižvelgiant į šias įžvalgas, būtina imtis veiksmų tiek teisėkūros, tiek praktinio įgyvendinimo srityse. Žemiau pateikiamos rekomendacijos, kurios, darbo autoriaus nuomone, galėtų padėti stiprinti privatumo apsaugą dirbtinio intelekto kontekste bei užtikrinti, kad technologijų plėtra vyktų žmogaus teisių apsaugos ribose:

1. Rekomenduojama kurti dialogą ir skatinti DI sistemų kūrėjus vadovautis ne tik teisiniais reikalavimais, bet ir etiniais principais, užtikrinant, kad privatumo apsauga būtų įdiegta jau technologijos kūrimo etape. Valstybė galėtų remti tokias iniciatyvas per inovacijų skatinimo programas ar teikti finansines paskatas etiškai atsakingiems technologijų kūrėjams.

2. Atsižvelgiant į tai, kad dažniausiai patys asmenys pateikia savo duomenis į skaitmeninę erdvę dėl neatsargumo ir mažo raštingumo informacinių technologijų srityje, rekomenduotina į nacionalinius skaitmeninio švietimo planus įtraukti aiškią edukacinę liniją apie tai, kaip saugiai naudotis socialiniais tinklais, kaip atpažinti profiliavimą ir kaip gintis nuo neteisėto duomenų naudojimo DI sistemose.

3. Dar iki galutinio DI akto įsigaliojimo rekomenduojama pradėti plačiau vertinti, kokias rizikas gali kelti dirbtinio intelekto naudojimas – tiek valstybės institucijose, tiek juridinių asmenų veiklose.

4. Atsižvelgiant į dirbtinio intelekto akto naujumą kol nėra aiškių akto taikymo praktikų ir rezultatų, ir į tai, kad šiuo metu Lietuvos Respublikoje nėra specializuoto teisės akto, reglamentuojančio dirbtinio intelekto technologijų keliamas grėsmes asmens privatumui, rekomenduojama inicijuoti ir priimti nacionalinį teisės aktą ar aiškius teisėkūros pakeitimus, kurie įtvirtintų DI sistemų atsakomybę ir pareigas privatumo apsaugos kontekste.

LITERATŪROS SĄRAŠAS

Teisės aktai:

1. Lietuvos Respublikos Konstitucija, žiūrėta 2025 m. kovo 26 d.

Įstatymai ir įstatymo galią turintys aktai

1. Lietuvos Respublikos baudžiamasis kodeksas, žiūrėta 2025 m. kovo 31 d.

Tarptautinės sutartys ir Europos sąjungos teisės aktai

1. Bendrasis duomenų apsaugos reglamentas, žiūrėta 2024 m. gruodžio 3 d.

2. Dirbtinio intelekto aktas, žiūrėta 2024 m. gruodžio 3 d. https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=OJ:L_202401689

3. Europos žmogaus teisių konvencija, žiūrėta 2024 m. gruodžio 3 d. https://www.echr.coe.int/documents/d/echr/convention_eng

4. Modernizuota Europos Tarybos Konvencija dėl asmens duomenų apsaugos (128-oji Ministrų Komiteto sesija, Elsinorė, 2018-05-17/18) https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016807c65bf%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Kiti teisės aktai

1. Europos Parlamentas, rezoliucija 2018/2855(RSP), žiūrėta 2025 m. balandžio 18 d. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52018IP0433&

2. ICO Enforcement notice (Jungtinės Karalystės Informacijos komisaro tarnyba), žiūrėta 2025 m. balandžio 14 d. https://ico.org.uk/media/action-weve-taken/enforcement-notices/4020437/clearview-ai-inc-en-20220518.pdf

3. ICO Monetary penalty notice, žiūrėta 2025 m. balandžio 14 d. https://ico.org.uk/media/action-weve-taken/mpns/4020436/clearview-ai-inc-mpn-20220518.pdf

Moksliniai šaltiniai:

1. A. F. Westin, „Privacy and Freedom“, žiūrėta 2024 m. gruodžio 4 d. https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr

2. A.M. Turing, „Mind a quarterly review of psychology and philosophy“, žiūrėta 2024 m. lapkričio 16 d.

3. Brendan Van Alsenoy, „Regulating data protection, the allocation of responsibility and risk among actors involved in personal data processing“, žiūrėta 2024 m. gruodžio 3 d. https://kuleuven.limo.libis.be/discovery/fulldisplay?docid=lirias1711667&context=SearchWebhook&vid=32KUL_KUL:Lirias&lang=en&search_scope=lirias_profile&adaptor=SearchWebhook&tab=LIRIAS&query=any,contains,LIRIAS1711667&offset=0

4. C. Smith, B. McGuire, T. Huang, G. Yang, „The History of Artificial Intelligence“, žiūrėta 2024 m. lapkričio 16 d. https://courses.cs.washington.edu/courses/csep590/06au/projects/history-ai.pdf
5. Christoper Mims, „A Powerful AI Breakthrough Is About to Transform the World“, žiūrėta 2024 m. lapkričio 28 d. https://www.wsj.com/tech/ai/a-powerful-ai-breakthrough-is-about-to-transform-the-world-095b81ea?
6. Goda Strikaitė-Latušinskaja, „Automatizuoti administraciniai nurodymai Lietuvoje“, žiūrėta 2025 m. kovo 14 d. https://www.zurnalai.vu.lt/teise/article/download/30836/29758?
7. Ikhlaq ur Rehman, „Facebook-Cambridge Analytica Data Harvesting: What You Need to Know“, žiūrėta 2025 m. balandžio 16 d. https://core.ac.uk/download/pdf/220153793.pdf
8. J. De Cew, „In Pursuit of Privacy“, žiūrėta 2024 m. gruodžio 4 d.
9. J. Holvast, „History of Privacy“, žiūrėta 2024 m. gruodžio 2 d. https://link.springer.com/chapter/10.1007/978-3-642-03315-5_2
10. J. McCarthy, M.L. Minsky, N. Rochester, C.E. Shannon, „A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence“, žiūrėta 2024 m. lapkričio 17 d. https://raysolomonoff.com/dartmouth/boxa/dart564props.pdf
11. John McCarthy, „What Is Artificial Intelligence?“, žiūrėta 2024 m. lapkričio 28 d. https://www-formal.stanford.edu/jmc/whatisai.pdf
12. Masahiro Morioka, „Descartes and Artificial Intelligence“, žiūrėta 2024 m. lapkričio 16 d. https://www.philosophyoflife.org/jpl2023si_intro.pdf
13.Mika Westerlund, „The Emergence of Deepfake Technology: A Review“, žiūrėta 2025 m. kovo 14d.https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf
14. Naveen Joshi, „7 Types of Artificial Intelligence“, žiūrėta 2024 m. gruodžio 2 d. https://www.forbes.com/sites/cognitiveworld/2019/06/19/7-types-of-artificialintelligence/?sh=45e12add233e
15. Nils J. Nilsson, „The Quest for Artificial Intelligence: A History of Ideas and Achievements“, žiūrėta 2024 m. lapkričio 28 d. https://ai.stanford.edu/~nilsson/QAI/qai.pdf
16. Omar Santos, Petar Radanliev, „Beyond the Algorithm: AI, Security, Privacy, and Ethics“, žiūrėta 2024 m. gruodžio 2 d. https://www.google.lt/books/edition/Beyond_the_Algorithm/QHriEAAAQBAJ?hl=lt&gbpv=0
17.Rui Hou, Diana Fu, „Sorting Citizens: Governing via China's Social Credit System“, žiūrėta 2025 m. kovo 14 d.

https://www.researchgate.net/profile/RuiHou2/publication/365862623_Sorting_citizens_Governing_via_China%27s_social_credit_system/links/6464f64a702026631653fff0/Sorting-citizens-Governing-via-Chinas-social-credit-system.pdf

18. S. Russel, P. Norvig, „Artificial Intelligence: A Modern Approach“, žiūrėta 2024 m. lapkričio 28 d. https://dl.ebooksworld.ir/books/Artificial.Intelligence.A.Modern.Approach.4th.Edition.Peter.Norvig.%20Stuart.Russell.Pearson.9780134610993.EBooksWorld.ir.pdf

19. Samuel D. Warren, Louis D. Brandeis, „The Right to Privacy“, žiūrėta 2024 m. gruodžio 3 d. https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf

20. W. Prosser, „California Law Review“, žiūrėta 2024 m. gruodžio 4 d. https://lawcat.berkeley.edu/record/1109651?v=pdf

21. W.A. Parent, „A New Definition of Privacy for the Law“, žiūrėta 2024 m. gruodžio 4 d. https://peeps.unet.brandeis.edu/~teuber/Parent_on_Privacy.pdf

22. Y. Lecun, Y. Bengio, G. Hinton, „Deep Learning“, žiūrėta 2024 m. lapkričio 17 d. https://hal.science/hal-04206682/document

Specialioji literatūra:

1. Cambridge dictionary, žiūrėta 2024 m. lapkričio 15 d. https://dictionary.cambridge.org/dictionary/english/automaton

2. K. Kardelis, „Mokslinių tyrimų metodologija ir metodai“, žiūrėta 2025 m. balandžio 10 d.

3. Lietuvių kalbos žodynas, žiūrėta 2024 m. lapkričio 15 d. https://www.lietuviuzodynas.lt/zodynas/Dirbtinis

4. Lietuvių kalbos žodynas, žiūrėta 2024 m. lapkričio 15 d. https://www.lietuviuzodynas.lt/zodynas/Intelektas

5. „Tyrimų metodai ir metodikos“, žiūrėta 2025 m. balandžio 10 d. https://mokslomedis.lt/atvejo-studija/

Teismų praktika:

1. EDPB „Decision by the Austrian SA against Clearview AI Infringements of Articles 5, 6, 9, 27 GDPR“, žiūrėta 2025 m. balandžio 14 d. https://www.edpb.europa.eu/news/national-news/2023/decision-austrian-sa-against-clearview-ai-infringements-articles-5-6-9-27_en

2. EDPB „Facial recognition: Italian SA fines Clearview AI EUR 20 million“, žiūrėta 2025 m. balandžio 14 d. https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

3. EDPB „Facial recognition: the French SA imposes a penalty payment on CLEARVIEW AI“, žiūrėta 2025 m. balandžio 14 d. https://www.edpb.europa.eu/news/national-news/2023/facial-recognition-french-sa-imposes-penalty-payment-clearview-ai_en

4. EDPB „Hellenic DPA fines Clearview AI 20 million euros“, žiūrėta 2025 m. balandžio 14 d. https://www.edpb.europa.eu/news/national-news/2022/hellenic-dpa-fines-clearview-ai-20-million-euros_en

5. First-tier Tribunal bylos nr. EA/20222/0165/FP, žiūrėta 2025 m. balandžio 14 d. https://www.bailii.org/uk/cases/UKFTT/GRC/2023/819.pdf

6. LR Konstitucinio teismo nutarimas „Dėl Lietuvos Respublikos Aukščiausiosios Tarybos 1991 m. sausio 31 d. nutarimo „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase“ atitikimo Lietuvos Respublikos Konstitucijai", žiūrėta 2025 m. kovo 31 d.

Internetiniai šaltiniai:

1. ACLU, „ACLU sues Clearview AI“, žiūrėta 2025 m. balandžio 11 d. https://www.aclu.org/press-releases/aclu-suesclearview-ai

2. AlexNet and ImageNet: The Birth of Deep Learning, žiūrėta 2024 m. lapkričio 15 d. https://www.pinecone.io/learn/series/image-search/imagenet/

3. Asmens duomenų apsauga, faktų apie Europos Sąjungą suvestinės, žiūrėta 2024 m. gruodžio 3 d. https://www.europarl.europa.eu/factsheets/lt/sheet/157/asmens-duomenu-apsauga

4. Australijos vyriausybės svetainė, „OAIC and UK's ICO open joint investigation into Clearview AI Inc.“, žiūrėta 2025 m. balandžio 11 d. https://www.oaic.gov.au/news/media-centre/oaic-and-uks-ico-open-joint-investigation-into-clearview-ai-inc.

5.„Bendras nacionalinių priemonių sąrašas“, žiūrėta 2025 m. balandžio 7 d. https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/nacionaliniu-priemoniu-sarasas/

6. Cambridge Analytica tinklalapio archyvas, žiūrėta 2025 m. balandžio 16 d. https://web.archive.org/web/20160216023554/https://cambridgeanalytica.org/services

7. Chart of signatures and ratifications of Treaty 108, žiūrėta 2024 m. gruodžio 3 d. https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108

8. CNIL „Restricted Committee Deliberation No. SAN-2022-019 of 17 October 2022 concerning CLEARVIEW AI“, žiūrėta 2025 m. balandžio 14 d. https://www.cnil.fr/sites/cnil/files/atoms/files/deliberation_of_the_restricted_committee_no_san-2022-019_of_17_october_2022_concerning_clearview_ai.pdf

9. CNIL „The CNIL‘s missions“, žiūrėta 2025 m. balandžio 11 d.
https://www.cnil.fr/en/cnil/cnils-missions
10. DSB, žiūrėta 2025 m. balandžio 11 d.
https://data-protection-authority.gv.at/#0
11. Europos duomenų apsaugos valdybos (EDAV) trisdešimt pirmoji plenarinė sesija..., žiūrėta 2025 m. balandžio 11 d.
https://www.edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_lt
12. Facial recognition: Italian SA fines Clearview AI EUR 20 million, žiūrėta 2025 m. kovo 18 d.
https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en
13. GPDP, „The Italian data protection authority: who we are“, žiūrėta 2025 m. balandžio 11 d.
https://www.garanteprivacy.it/web/garante-privacy-en/the-italian-data-protection-authority-who-we-are
14. Google Duplex: An AI System for Accomplishing Real-World Tasks Over the Phone, žiūrėta 2024 m. lapkričio 16 d.
https://research.google/blog/google-duplex-an-ai-system-for-accomplishing-real-world-tasks-over-the-phone/
15. “Google trends” duomenys, žiūrėta 2024 m. lapkričio 15 d.
https://trends.google.com/trends/explore?date=today%205-y&q=artificial%20intelligenc&hl=en-GB
16. HDPA „Mission“, žiūrėta 2025 m. balandžio 11 d.
https://www.dpa.gr/en/hdpa/mission
17. „How Amazon is using generative AI to improve product recommendations and descriptions“, žiūrėta 2024 m. lapkričio 28 d.
https://www.aboutamazon.com/news/retail/amazon-generative-ai-product-search-results-and-descriptions
18. IBM History „Deep blue“, žiūrėta 2025 m. gruodžio 2 d.
https://www.ibm.com/history/deep-blue
19.ICO „Information Commissioner seeks permission to appeal Clearview AI Inc ruling“, žiūrėta 2025 m. balandžio 14 d.
https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2023/11/information-commissioner-seeks-permission-to-appeal-clearview-ai-inc-ruling/

20. ICO „Investigation into the use of data analytics in political campaigns“, žiūrėta 2025 m. balandžio 18 d.
https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf
21. ICO „Our work on Artificial Intelligence“, žiūrėta 2025 m. balandžio 11 d.
https://ico.org.uk/about-the-ico/what-we-do/our-work-on-artificial-intelligence/
22. IMY (Sweden) - DI-2020-2719, žiūrėta 2025 m. balandžio 11 d.
https://gdprhub.eu/index.php?title=IMY_(Sweden)_-_DI-2020-2719
23. Jungtinės Karalystės vyriausybės svetainė „Information Commissioner's Office“, žiūrėta 2025 m. balandžio 11 d.
https://www.gov.uk/government/organisations/information-commissioner-s-office
24. Kashmir Hill, „The Secretive Company That Might End Privacy as We Know It“, žiūrėta 2025 m. balandžio 10 d.
https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
25. „Landmark judgments“, žiūrėta 2024 m. gruodžio 3 d.
https://www.coe.int/en/web/human-rights-convention/landmark-judgments
26.„Laiko juosta – DI akto įsigaliojimas ir pagrindiniai įsipareigojimai“, žiūrėta 2025 m. balandžio 7 d.
https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/laiko-juosta/
27. Oxford Essential Quotations, žiūrėta 2024 m. gruodžio 3 d.
https://www.oxfordreference.com/display/10.1093/acref/9780191826719.001.0001/q-oro-ed4-00003117?
28. RunSensible’s Legal Dictionary, žiūrėta 2024 m. gruodžio 3 d.
https://www.runsensible.com/legal-dictionary/domus-sua-cuique-est-tutissimum-refugium/
29. Stanford encyclopedia of philosophy archive „Privacy“, žiūrėta 2024 m. gruodžio 2 d.
https://plato.stanford.edu/archives/spr2018/entries/privacy/
30. „The Applications of AI in Natural Language Processing, Computer Vision, and Speech Recognition“, žiūrėta 2024 m. gruodžio 2 d.
https://futureskillsprime.in/knowledge-center/tech-simplified/applications-ai-natural-language-processing-computer-vision-and-speech-recognition

31. “The European Convention on Human Rights - how does it work?”, žiūrėta 2024 m. gruodžio 3 d. https://www.coe.int/en/web/impact-convention-human-rights/how-it-works
32. „The story of Talos“, žiūrėta 2024 m. lapkričio 15 d. https://eurekacourses.org/the-story-of-talos/
33. The Washington Post „A face-scanning algorithm increasingly decides whether you deserve the job“, žiūrėta 2025 m. kovo 18 d. https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/
34. „We are Clearview AI“, žiūrėta 2025 m. balandžio 10 d. https://www.clearview.ai/overview
35. „What is the history of artificial intelligence?“, žiūrėta 2024 m. lapkričio 17 d. https://www.tableau.com/data-insights/ai/history
36. „Žmogaus teises ginančių institucijų sąrašas“, žiūrėta 2025 m. balandžio 7 d. https://eimin.lrv.lt/lt/veiklos-sritys/skaitmenine-politika/dirbtinis-intelektas/di-akto-igyvendinimas/zmogaus-teises-ginancios-istaigos/

SANTRAUKA LIETUVIŲ KALBA

Šiame magistro baigiamajame darbe, autoriaus analizuojama, kaip dirbtinio intelekto technologijų taikymas veikia asmens teisės į privatumą apsaugą šiuolaikinėje visuomenėje. Atsižvelgiant į tai, kad DI sistemų galimybės sparčiai plečiasi ir tampa vis labiau integruotos į kasdienį gyvenimą, didėja rizika asmens duomenų saugumui bei privatumo pažeidimams. Pagrindinis darbo tikslas – išnagrinėti dirbtinio intelekto technologijų praktikoje keliamas grėsmes asmens teisės į privatumą apsaugai ir įvertinti esamą teisinį reguliavimą, siekiant nustatyti jo tinkamumą šių grėsmių kontekste.

Teorinėje darbo dalyje išanalizuota dirbtinio intelekto samprata, raida, klasifikacija bei pagrindinės savybės, taip pat aptarta asmens teisės į privatumą raida nuo filosofinių ištakų iki šiuolaikinio reglamentavimo. Nagrinėti Europos Sąjungos ir nacionalinės teisės aktai, įskaitant Europos žmogaus teisių konvenciją, Bendrąjį duomenų apsaugos reglamentą, didelis dėmesys buvo skiriamas Dirbtinio intelekto aktui. Empirinėje dalyje taikyta atvejo studijos metodika, nagrinėjant įmonių „ Clearview AI“ ir „Cambridge Analytica“ pavyzdžius. Šių atvejų tyrimas leido išryškinti DI keliamas grėsmes teisei į privatumą praktikoje ir įvertinti padarytus pažeidimus bei institucijų reakcijas.

Atliktas tyrimas patvirtino, kad grėsmė privatumo apsaugai kyla ne iš pačios DI technologijos, bet iš būdo, kuriuo ji taikoma. Nustatyta, jog naujasis Europos Sąjungos Dirbtinio intelekto aktas yra reikšmingas žingsnis užtikrinant asmens duomenų apsaugą, taip pat teisę į privatumą sustiprina Bendrasis duomenų apsaugos reglamentas, tačiau siekiant efektyvios apsaugos būtina stiprinti ir vartotojų sąmoningumą, ir technologijų kūrėjų atsakomybę.

SUMMARY

In this master's thesis, the author analyzes how the application of artificial intelligence (AI) technologies affects the protection of the right to privacy in contemporary society. Given that the capabilities of AI systems are rapidly expanding and becoming increasingly integrated into everyday life, the risks to personal data security and privacy violations are growing. The main objective of the thesis is to examine the threats posed by the practical use of AI technologies to the protection of the right to privacy and to assess the current legal framework in order to determine its adequacy in the context of these threats.

The theoretical part of the thesis analyzes the concept, development, classification, and key characteristics of artificial intelligence, as well as the evolution of the right to privacy from philosophical origins to modern regulation. The analysis includes European Union and national legal acts, including the European Convention on Human Rights and the General Data Protection Regulation (GDPR), with significant attention given to the Artificial Intelligence Act. The empirical part applies the case study method, analyzing the examples of the companies "Clearview AI" and "Cambridge Analytica". The analysis of these cases highlights the threats that AI poses to the right to privacy in practice and evaluates the violations committed and the responses of relevant institutions.

The conducted research confirms that the threat to privacy protection arises not from the AI technology itself but from the way it is applied. It was found that the new Artificial Intelligence Act of the European Union is a significant step in ensuring the protection of personal data. Furthermore, the GDPR also strengthens the right to privacy. However, to achieve effective protection, it is essential to enhance both consumer awareness and the accountability of technology developers.