Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Adriano Latvinsko,
V kurso, Tarptautinės ir Europos Sąjungos teisės
studijų šakos studento

Magistro darbas

Duomenų apsaugos ir dirbtinio intelekto suderinamumas: BDAR, ES DI aktas, CCPA ir kiti aktualūs teisės aktai

Data protection and AI compatibility: GDPR, EU AI Act, CCPA and other relevant legislation

Vadovė: asist. dr. Neringa Gaubienė

Recenzentė: asist. dr. Laura Paškevičienė

Vilnius
2025

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe nagrinėjamas bendrosios paskirties dirbtinio intelekto (BPDI) sistemų suderinamumas su aktualiu duomenų apsaugos reguliavimu, daugiausiai dėmesio skiriant BDAR, ES dirbtinio intelekto aktui ir CCPA. Darbe kritiškai nagrinėjama, kaip BPDI modeliai renka, tvarko ir daro išvadas apie duomenų subjektus ir jų duomenis, vertinami dėl to kylantys teisiniai, etiniai ir techniniai iššūkiai. Pasitelkiant lyginamąją teisinę analizę, vadovaujantis institucijų rekomendacijomis ir teismų sprendimais, darbe nustatomos JAV ir ES jurisdikcijų reguliavimo spragos ir siūloma adaptuoti įstatymus, skiriant prioritetą duomenų subjektų teisėms, atsakomybei ir atitikčiai BPDI atžvilgiu stiprinti.

Pagrindiniai žodžiai: asmens duomenų apsauga, bendrosios paskirties dirbtinis intelektas, dideli kalbos modeliai, ES bendrasis duomenų apsaugos reglamentas, Kalifornijos vartotojų privatumo teisės aktas.

The work examines the compatibility of general-purpose artificial intelligence (GPAI) systems with relevant data protection regulation, focusing on the GDPR, the EU AI Act and the CCPA. The work critically examines how BPDI models collect, process and infer data about data subjects and their data, and assesses the legal, ethical and technical challenges this poses. Using comparative legal analysis, guided by institutional recommendations and court decisions, the paper identifies regulatory gaps in the US and EU jurisdictions and proposes adaptations to the law, prioritizing the rights, responsibilities and compliance of data subjects in relation to BPDI.

Keywords: personal data protection, general-purpose artificial intelligence, large language models, EU General Data Protection Regulation, California Consumer Privacy Act.

TURINYS

SANTRUMPŲ SARAŠAS

BPDI – bendrosios paskirties dirbtinis intelektas;

ES – Europos Sąjunga;

JAV – Jungtinės Amerikos Valstijos;

BDAR - Europos Sąjungos bendrasis duomenų apsaugos reglamentas;

CCPA (angl. *California Consumer Privacy Act*) - Kalifornijos vartotojų privatumo teisės aktas;

ES DI aktas - Europos Sąjungos dirbtinio intelekto aktas;

LLM (angl.: *Large Language Model*) - didelis kalbos modelis;

CPRA (angl.: *California Privacy Rights Act)* - Kalifornijos privatumo teisių aktas.

ĮVADAS

Šiuolaikiniame pasaulyje, kur skaitmeninės technologijos daro įtaką kone kiekvienam mūsų gyvenimo aspektui, duomenų apsauga ir dirbtinio intelekto (toliau – „**DI**“) plėtra tampa neatsiejamomis ir viena kita tiesiogiai veikiančiomis sritimis. Ypač aktualus tampa bendrosios paskirties dirbtinis intelektas (toliau „**BPDI**“), kuris būdamas pažangiausiu ir plačiausiai prieinamu DI tipu, sparčiai keičia įvairias žmonijos veiklos sritis - nuo privataus naudojimo kūrybai ar pramogoms iki komercinio įgalinimo verslo ar viešojo sektoriaus reikmėms. Šiandien BPDI yra ne tik futuristinė technologinė naujovė, kaip kvantiniai kompiuteriai bei kiti robotikos pažadai su siauromis pritaikymo galimybėmis, bet ir galingas geopolitikos bei visuomenės tendencijas formuojantis įrankis, kurio naudojimo mastas su kiekviena diena sparčiai auga. Vis didėjanti BPDI integracija, beveik kiekvieno žmogaus gyvenime neretai yra įtakojama baimės atsilikti ir (ar) praleisti naujas galimybes, naujus potencialus, kuriuos žada ši technologija (angl.: fear of missing out).

Auganti žmonijos priklausomybė kibernetinėms technologijoms, įskaitant ir tas, kurių naudojimas kvestionuoja moralės normas (pvz.: SilkRoad, DarkWeb, Paragon Graphity, tai yra Izrealio šnipinėjimo sistema, Signal, tai yra privatus Messenger, su šifruota informacija, kuri riboja teisėsaugos prieigą, Cambridge Analytica ir kiti variantai), ir vis tobulinami DI algoritmai, skirti pritraukti kuo įmanoma ilgesniam laikotarpiui vartotojų dėmesį ir įgalinantys vartotoją priimti kuo mažiau pastangų reikalaujančius sprendimus, bet ne visada saugiausius, kelia rimtų iššūkių asmens duomenų apsaugai. Įprasti BPDI vartotojai, dažnai nesusimąstydami, sukelia masyvius asmeninės informacijos kiekius (angl.: data points) į didelių kalbos modelių (toliau – „**LLM**“) sistemas ir taip neakivaizdžiai patiki savo duomenimis BPDI rinkos lyderiams, o tai savaime didina šių asmenų privatumo pažeidžiamumo riziką. Šiame kontekste neatsitiktinai naudojami žodžiai "neakivaizdžiai patiki", kadangi BPDI modelius valdančios kompanijos įvairiausiais būdais bando paslėpti savo tikruosius informacijos naudojimo tikslus, sumenkinti mokslininkų tyrimus, atskleidžiančius jog šifruotos informacijos bitai gali būti sujungti į vieną visumą. Kitaip tariant net ir šifruota, aukščiausius saugumo kriterijus atitinkanti informacija gali padėti įsilaužėliams identifikuoti pavienius vartotojus. Duomenų apsauga ir bendrai kibernetinis saugumas šioje sparčiai besivystančioje aplinkoje tampa itin opia problema, nes tobulėjant technologijoms kartu tobulėja įrankiai palengvinantys įsilaužėlių darbą. Tai nors DI gali padėti atremti kibernetines atakas efektyviau, o BPDI netgi padėti sukurti apsaugines sistemas, tačiau vis tobulėjant mechanizmams, lygiagrečiai tobulėja ir

įsilaužėlių priemonės, kas lemia jog DI technologijos tampa patraukliu taikiniu potencialioms įsilaužėlių atakoms.

Temos aktualumas. Remiantis aukščiau išvardintomis tendencijomis, darosi akivaizdu, jog būtina išsamiai analizuoti, kaip BPDI sistemos atitinka galiojančius duomenų apsaugos ir DI teisės aktus. Itin svarbu yra plėtoti diskusiją ar dabartiniai teisės aktai Europos Sąjungos (toliau – „**ES**“) ir Jungtinių Amerikos Valstijų (toliau – „**JAV**“) lygiu yra pakankami reguliuoti sparčiai besivystantį BPDI, užtikrinti asmens duomenų apsaugą ir atsakomybę už įstatymų pažeidimus. Dėl įvairiapusiškos problematikos DI kontekste šiame magistro darbe koncentruojamasi būtent į ES – Bendrąjį duomenų apsaugos reglamentą (toliau – „**BDAR**“) ir Europos Sąjungos dirbtinio intelekto aktą (toliau – „**ES DI aktas**“) ir JAV – Kalifornijos vartotojų privatumo įstatymą (toliau – „**CCPA**“). Pagrindiniai akcentai dedami ties teisinio reguliavimo kertiniais principais ir aktualiomis įstatymų normomis, siekiant nustatyti, kaip šios skirtingos teisės tradicijos veikia BPDI vystymosi, integracijos ir naudojimo procesus. Tyrimo metu bus siekiama ne tik apžvelgti esminius teisės aktų principus, tai yra teorinį lygmenį, bet ir išsiaiškinti praktinius jų taikymo iššūkius, atsakomybės paskirstymo klausimus bei galimus konfliktus tarp skirtingų jurisdikcijų. Galiausiai, remiantis atlikta analize, bus pateiktos rekomendacijos, galinčios prisidėti prie BPDI teisinio reguliavimo tobulinimo ir praktinio atitikties užtikrinimo, atsižvelgiant į technologijų specifiką, regioninius skirtumus ir etinius aspektus. Didelis duomenų kiekis talpinamas LLM sistemose, vis populiarėjanti BPDI integracija, šių sistemų veikimo principai ir inicijuoti teisiniai bylinėjimai prieš DI rinkos lyderius lemia, kad šis tyrimas yra aktualus tiek teoriniu, tiek praktiniu požiūriu, siekiant užtikrinti tinkamą asmens duomenų apsaugą ir sąžiningą bei atsakingą DI vystymąsi.

Darbo tikslas: Išsamiai išnagrinėti ir įvertinti BPDI sistemų atitiktį ES ir JAV duomenų apsaugos bei dirbtinio intelekto teisės aktams.

Darbo uždaviniai. Tinkamas magistro darbo temos atskleidimas ir tikslo įgyvendinimas reikalauja:

- Apžvelgti esminius BDAR, ES DI akto ir CCPA principus, susijusius su duomenų apsauga ir BPDI reguliavimu;
- Išsiaiškinti, kaip BPDI sistemos, tokios kaip LLM, atitinka BDAR ir CCPA reikalavimus, būtent didžiausią dėmesį skiriant duomenų rinkimui, tvarkymui ir naudojimui;

- Išnagrinėti duomenų valdytojo ir duomenų tvarkytojo atsakomybės paskirstymo klausimus BPDI sistemų sukūrimo, apmokymo ir integracijos procesuose, identifikuojant galimas atsakomybės spragas;
- Apžvelgti praktinių situacijų stipriąsias ir silpnąsias puses, naudojantis tarptautinių ir nacionalinių teismų praktika bei duomenų apsaugos institucijų nurodymais;
- Išskirti pagrindinius iššūkius, kylančius dėl skirtingų ES ir JAV teisės aktų ir jų taikymo BPDI, analizuojant galimus konfliktus ir neaiškumus tarptautiniu mastu;
- Pateikti rekomendacijas dėl BPDI teisinio reguliavimo tobulinimo ir praktinio atitikties užtikrinimo, atsižvelgiant į technologijų specifiką, regionų skirtumus ir etinius aspektus.

Objektas. Asmens duomenų apsaugos ir BPDI suderinamumas. Magistro darbe siekiama analizuoti būtent, dabartiniu metu labiausiai išvystyto ir žmonijos rasei prieinamo BPDI atitiktį ES ir JAV duomenų apsaugos bei dirbtinio intelekto teisės aktams.

Tyrimo metodai. Siekiant visapusiškai atskleisti temą, šiame magistro darbe pasitelkiami šie kiekybiniai ir teoriniai metodai:

- Lyginamasis metodas - taikytas bandant surasti sutapimus ir atskleisti skirtumus tarp ES ir JAV galiojančių teisės aktų, būtent duomenų apsaugos ir DI srityje.
- Analitinis - kritinis metodas - pritaikomas analizuojant duomenų apsaugą ir DI reguliavimo klausimus, juos išskaidant į smulkesnes potemes, o tai įgalina formuoti objektyvią kritiką įstatymų leidėjams;
- Metaanalizės metodas - naudojamas siekiant atskleisti bendrą, unifikuotą mokslininkų poziciją dėl duomenų apsaugos reikalavimų laikymosi LLM, išnagrinėti institucijų rekomendacijas dėl LLM atitikties teisės aktams, įvardinti lyderiaujančių kompanijų pozicijas dėl teisinio reglamentavimo įgyvendinimo;
- Statistinė analizė - naudojama susisteminti duomenims, išskirti pasikartojančius dėsningumus DI naudojimo praktikose;
- Teisės informatikos metodas - analizuojama kaip LLM daro įtaką teisinių problemų sprendimuose, kokios grėsmės kyla dėl DI integravimo teisinių duomenų bazėse;
- Istorinis metodas - atskleidžiama teisinio reglamentavimo formavimosi raida dėl nuolatos tobulėjančio DI, gerosios ir blogosios praktikos;
- Analogijos metodas - remiantis įsigaliojusiais teismų sprendimais, specialistų bei duomenų apsaugos institucijų nuomonėmis, priimtais teisės aktais, formuojamos bei taikomos teisės normos tebesivystančiam BPDI;

- Teisinių dokumentų analizės metodas - pritaikytas renkant, sisteminant ES ir JAV teisinius dokumentus, teismų išvadas;

Darbo originalumas. Nėra kvestionuojama, kad šis magistro darbas yra originalus savo išsikeltais uždaviniais, pasirinktų atvejų analize ir įvardintu tikslu, nes jame siekiama ne tik apžvelgti esamas BDAR ir ES DI akto bei CCPA duomenų apsaugos ir dirbtinio intelekto reguliavimo normas, bet taip pat atlikti giluminę analizę, kaip skirtingos jurisdikcijos veikia šiuolaikinio BPDI vystymąsi, integraciją ir naudojimą. Skirtingai nuo autoriui žinomų akademinių darbų, kurie įprastai apsiriboja tik atskirų teisės aktų analize ar susitelkia tik į bendrų principų paieškas, ar nagrinėja tiktai teorinius aspektus, šis magistro darbas koncentruojasi ne tik į teorinius kazusus, bet ir į praktinius BPDI sistemų atitikties ES ir JAV teisės aktams iššūkius. Nors darbe analizuojami ganėtinai plačiai aptarinėjami duomenų rinkimo, tvarkymo ir naudojimo aspektai, taip pat atsakomybės paskirstymas BPDI kontekste, atsižvelgiant į teismų praktiką, tačiau į šiuos kriterijus stengiamasi pažvelgti iš kitos perspektyvos. Tokia strategija yra siekiama identifikuoti ES ir JAV teisės aktų taikymo BPDI atžvilgiu konfliktus bei išskirti konkrečias teisinio reguliavimo tobulinimo rekomendacijas, atsižvelgiant į technologijų specifiką ir etinius aspektus. Būtent kompleksinis požiūris, apjungiantis teorinę analizę su praktiniais BPDI taikymo iššūkiais ir galimais skirtingų jurisdikcijų tarpusavio konfliktais, bei siekis pateikti praktiškai integruojamas rekomendacijas, kiekvieną dieną besikeičiančiam BPDI, suteikia šiam darbui originalumo.

Svarbiausi šaltiniai ir literatūra. Neabejotina, kad šiame magistro darbe svarbiausi šaltiniai yra teisės aktų rinkiniai kaip BDAR, ES DI aktas, CCPA, kurie yra kertiniai įrankiai suprasti įstatymų leidėjų ketinimus, atskleisti teisinio reguliavimo vystymosi spartą ir problematiką. Nors yra mokslinių bei magistro darbų rašytų panašiomis temomis, kaip Kavoliūnaitės-Ragauskienės, Eglės „Teisė į privatumą, asmens duomenų apsauga ir dirbtinis intelektas: teisinio reguliavimo iššūkiai Lietuvoje ir Europoje“; Malakausko, Arno „Automatizuotas sprendimų priėmimas pagal BDAR 22 straipsnį ir dirbtinis intelektas: taikymo prielaidos ir problematika“, tačiau šiuose darbuose diskutuojama apie DI kaip visumą ir neapimama BPDI arba susitelkiama tik į ES reguliavimą, arba vertinamas tik vienas ar keli iš aspektų įvertintų šiame magistro darbe, bet neapžvelgiami visi kartu. Kadangi darbe yra fokusuojamasi į duomenų apsaugą ir BPDI suderinamumą teoriniame ir praktiniame lygmenyje, tai itin svarbūs yra ne tik tarptautinių ir nacionalinių teismų, patenkančių į nagrinėjamų jurisdikcijų ribas, sprendimai, bet ir pripažintų duomenų apsaugos institucijų kaip Europos skaitmeninių teisių centras (angl.: NOYB), Italijos (ital.:

Garante), Prancūzijos (pran.: CNIL), Airijos (angl.: DPC) bei Vokietijos (vok.: BfDI), Lenkijos (lenk.: UODO), Europos duomenų apsaugos valdyba (angl.: EDPO) rekomendacijos, apžvalgos ir priimti sprendimai. Atsižvelgiant į oficialios BDAR, ES DI akto bei CCPA aiškinimo praktikos trūkumą BPDI klausimais, plačiai remiamasi specialiąja literatūra, kaip Europos ir JAV autoritetingų mokslininkų įžvalgomis, tai yra – Wang, T., Wachter, S., Vaele, M., Barbera, I., Cartwright, O., Cheong, B. C., Pahune, S. bei kiti. Taip pat vieni esminių šaltinių ir dažnai naudojami yra J. Zaleskio monografija „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“ bei C. Kuner knyga „The EU General Data Protection Regulation (GDPR): A Commentary“.

1. GENERATYVINIS DIRBTINIS INTELEKTAS IR DUOMENŲ APSAUGA: ES IR JAV TEISINIŲ SISTEMŲ LYGINAMOJI ANALIZĖ

Pastarojo dešimtmečio technologinis proveržis, suteikiantis vis didesniam asmenų kiekiui galimybę turėti prieigą prie interneto net ir tolimiausiuose regionuose, didėjančios žmonių galimybės sukurti pajėgesnius techninius sprendimus, pritaikyti skaitmeninius įrankius kasdieninių užduočių atlikimui ir sparčiais tempais tobulėjantis dirbtinis intelektas, lėmė BPDI sistemų eksponentinę pažangą (Storey et al., 2025). Spartus bendrosios paskirties BPDI atsiradimas sukėlė didelį spaudimą abiem jurisdikcijoms, paskatinęs tiek ES, tiek JAV iš naujo įvertinti savo duomenų apsaugos įstatymus. Pagrindiniai šio skyriaus akcentai yra BDAR, ES DI aktas, o JAV - CCPA kartu su Kalifornijos privatumo teisių aktu (toliau – „**CPRA**“). Šios dvi jurisdikcijos atspindi iš esmės skirtingas teisines tradicijas - ES teisėje akcentuojamos pagrindinės teisės ir centralizuotą priežiūrą, o JAV reguliavime linkstama vadovautis rinka grindžiamu ir decentralizuotu požiūriu. Nepaisant struktūrinių skirtumų, abiejose sistemose stengiamasi pateikti reguliavimo atsaką į eksponentinį BPDI augimą ir su tuo susijusius duomenų valdymo iššūkius.

1.1. ES DUOMENŲ APSAUGOS TEISĖS PRINCIPAI IR JŲ TAIKYMAS BENDROSIOS PASKIRTIES DIRBTINIAM INTELEKTUI

2016 m. priimtame ir nuo 2018 m. įgyvendinamame BDAR nustatomi griežti su asmens duomenimis susiję principai ir asmens teisės. Šie principai - teisėtumo, sąžiningumo, skaidrumo, tikslo apribojimo, duomenų kiekio mažinimo, tikslumo, saugojimo apribojimo, konfidencialumo ir atsakomybės - yra pamatiniai atliekant bet kokį BPDI sistemos atitikties vertinimą (BDAR, 5 straipsnis). Tačiau praktinis šių principų taikymas BPDI atskleidžia rimtų sunkumų. Pavyzdžiui, pagal BDAR 13 straipsnyje nustatytus skaidrumo reikalavimus reikalaujama aiškiai informuoti apie duomenų tvarkymo praktiką, tačiau daugelis BPDI kūrėjų neatskleidžia, kaip ir iš kur gaunami duomenys naudojami mokymo tikslais, taip apribodami naudotojų galimybes prieš duodant sutikimą būti tinkamai informuotais (Zaleskis, 2019). Panašiai, tikslo ribojimo principas dažnai pažeidžiamas, kai iš viešai prieinamų šaltinių surenkami duomenys yra pertvarkomi tokioms programoms, kaip asmens elgsenos profiliavimas, adaptuoto turinio generavimas ar biometrinė analizė (Sarra, 2023). Be to, duomenų apribojimą sunku įgyvendinti, nes BPDI remiasi didžiuliais ir nevienalyčiais duomenų rinkiniais, kurie daugelyje atvejų yra laikomi pavieniais ir todėl

nereikalingais arba netiesiogiai identifikuojančiais asmens duomenis. Galiausiai, tokios teisės kaip galimybė sužinoti, ištrynimas ar ištaisymas (BDAR 15-21 straipsniai) tampa techniškai neįgyvendinamos tokiose situacijose, nes naudotojo duomenys iš esmės yra įterpti į modelio svorius, todėl jų atskyrimas ir pašalinimas praktiškai neįmanomas (CNIL, 2023).

Siekdama papildyti BDAR ir spręsti su dirbtiniu intelektu susijusią riziką, ES priėmė DI aktą - plataus užmojo reguliavimo sistemą, kuri šiuo metu tobulinama ir galutinę stadiją turėtų pasiekti 2026 metais. Priimtame įstatyme siūloma keturių lygių, rizika pagrįsta klasifikavimo sistema, kurią būtų galima skaidyti į šias dalis: nepriimtina, didelė, ribota ir minimali rizika. Tikėtina, kad BPDI modeliai, ypač LLM, atsižvelgiant į jų apmokymo kontekstą, bus priskiriami bendrosios paskirties, arba didelės rizikos sistemoms. Toks požiūris susidaro, vertinant, kad didelės rizikos klasifikavimas taikomas tokiuose sektoriuose kaip sveikatos priežiūra, švietimas, įdarbinimas ir teisėsauga - srityse, kuriose sisteminis šališkumas, ydingi rezultatai ar diskriminacinė praktika gali daryti didelį poveikį pagrindinėms teisėms (Sarra, 2023). Rizikos priskyrimas priklauso nuo numatomos funkcijos, galimo poveikio ir naudojimo konteksto, tai yra pagrindiniai kriterijai į kuriuos reikia atsižvelgti. Tai itin svarbu, nes ES DI akte nustatyti griežti įpareigojimai didelės rizikos sistemoms, įskaitant dokumentavimą, žmogiškąją priežiūrą, patikimumo testavimą, skaidrumo priemones ir stebėseną po išleidimo į rinką (Lyu, 2023). Šios pastangos atspindi ES įsipareigojimą laikytis atsargumo principo, tačiau mokslininkai įspėja, kad atitikties užtikrinimas, ypač dėl BPDI sistemų neskaidraus veikimo, gali būti technologiškai ir administraciniu požiūriu sudėtingas.

1.2. JAV DUOMENŲ APSAUGOS TEISĖS AKTŲ PRINCIPAI IR JŲ TAIKYMAS BENDROSIOS PASKIRTIES DIRBTINIAM INTELEKTUI

Priešingai nei ES suvienodintas duomenų apsaugos teisinis rėžimas, JAV nėra vieno suderinto federalinio privatumo įstatymo, kadangi duomenų apsauga reglamentuojama fragmentiškai, valstijų lygmeniu. 2018 m. priimtas CCPA ir jį papildantis CPRA, įsigaliojęs nuo 2023 m., yra išsamiausi duomenų apsaugos įstatymai JAV lygmeniu. Šiais įstatymais gyventojams suteikiamos kelios pagrindinės teisės, tai yra susipažinti su apie juos surinkta asmenine informacija, prašyti ją ištrinti, uždrausti jos pardavimą trečiosioms šalims ir reikalauti ištaisyti netikslią informaciją (Bloomberg Law, 2023). CPRA priėmimo dėka buvo įsteigta Kalifornijos privatumo apsaugos agentūra, kuriai pavesta užtikrinti

BPDI atitiktį norminiam reguliavimui ir jo vykdymą. Nepaisant šių svarbių pasiekimų, BPDI iškyla nemažai teisinių iššūkių, kurie patikrina tokių teisių įgyvendinimą praktikoje ir veiksmingumą. BPDI sistemos įprastai apdoroja didelius kiekius asmeninių ir žmogaus įpročius formuojančių duomenų, kad sukurtų prognozes ir rezultatus, dažnai tai darydamos be duomenų subjektų žinios ar sutikimo. Kaip pažymima NYU intelektinės nuosavybės ir pramogų teisės žurnale (2024 m.), naudotojai dažnai nežino, kad jų duomenys, įvesti į dirbtinio intelekto platformas, yra saugomi ir naudojami modelio elgsenai tobulinti. Net jei naudotojai žino, techninė BPDI modelių architektūra dažnai neleidžia veiksmingai pasinaudoti tokiomis teisėmis kaip informacijos apie subjektą ištrynimas ar ištaisymas, nes pasitelkus asmens duomenis apmokymo tikslams, jie tampa neatskiriama LLM sistemos dalimi.

Prie šių apribojimų prisideda ir reguliavimo sistemos struktūriniai trūkumai. Pagrindiniai duomenų apsaugos principai, tokie kaip tikslo apribojimas ir duomenų kiekio mažinimas, nors ir atsispindi CPRA, vis dar sunkiai įgyvendinami BPDI kontekste dėl mokymo duomenų apimties ir pobūdžio. Mokslininkai teigia, kad išvestiniai ir apibendrinti duomenys - dažnai naudojami BPDI sistemose - dažnai nepatenka į teisės aktais nustatytas "asmens duomenų" apibrėžtis, todėl kūrėjai gali išvengti tiesioginių teisinių prievolių (Koene, Palmer, 2022). Kaip rodo Lyu (2023), BPDI paslaugų teikėjai retai diegia mechanizmus, leidžiančius naudotojams suprasti, kaip buvo naudojami jų duomenys, arba įgyti teisę prašyti pašalinti išvestines LLM modelių išvadas. Tuo tarpu, nors CPPA buvo sukurta siekiant sustiprinti vykdymo užtikrinimą, jos operatyviniai pajėgumai tebėra riboti tiek išteklių, tiek technologinės kompetencijos požiūriu (IAPP, 2024). Padėtį dar labiau apsunkina reguliavimo fragmentiškumas: kitos valstijos, pavyzdžiui, Virdžinija, Koloradas ir Juta, priėmė siauros apimties privatumo įstatymus, kurie nėra tokie išsamūs kaip Kalifornijos duomenų apsaugos teisės aktai. Šis skirtingumas apsunkina nuoseklumą nacionaliniu lygmeniu ir kenkia tarpvalstybinei sąveikai su tarptautinėmis sistemomis, pavyzdžiui, BDAR. Pasak Sarra (2023), toks reguliavimo disonansas trukdo pasauliniam duomenų valdymui ir kelia netikrumą skirtingose jurisdikcijose veikiančių BPDI priemonių kūrėjams. Nors CCPA ir CPRA yra pamatinis žingsnis link dirbtiniam intelektui pritaikyto privatumo valdymo, jų pajėgumas apsaugoti duomenų subjektų teises realiose BPDI taikomosiose programose išlieka struktūriškai ir funkciškai ribotas.

1.3. ASMENS DUOMENŲ SĄVOKOS APIBRĖŽIMAS IR DUOMENŲ KATEGORIJOS BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO KONTEKSTE

Kartu su sparčiai vystomu BPDI, atsirado naujų asmens duomenų teisinio tvarkymo aspektų. Nors ši technologija suteikia galingų galimybių - nuo į žmogų panašaus teksto generavimo iki vaizdų sintezės, programavimo kodų ir prognozių - ji kartu kelia iššūkių nusistovėjusioms duomenų apsaugos sistemoms. Tiek ES, tiek JAV bandė reaguoti į šiuos pokyčius, nors jų teisinės sistemos skiriasi savo struktūra, taikymo sritimi ir pagrindinėmis filosofijomis. Visų pirma tokios kategorijos kaip specialūs arba neskelbtini asmens duomenys, išvestiniai duomenys, pseudoniminiai duomenys ir anoniminiai duomenys įgauna naują svarbą BPDI kontekste. Norint įvertinti atitikties riziką ir nustatyti reguliavimo spragas, labai svarbu suprasti, kaip šios kategorijos aiškinamos, tvarkomos ir reguliuojamos tiek ES, tiek JAV.

Pagal Bendrojo duomenų apsaugos reglamento (BDAR) 9 straipsnį ES tam tikrų rūšių informaciją, pavyzdžiui, rasinę ar etninę kilmę, religinius įsitikinimus, duomenis apie sveikatą ar seksualinę orientaciją, priskiria specialioms asmens duomenų kategorijoms, kurioms reikia didesnės apsaugos. Juos tvarkyti draudžiama, išskyrus atvejus, kai tai aiškiai pagrįsta, pavyzdžiui, duomenų subjekto sutikimu arba įrodžius, kad tai būtina viešajam interesui. Priešingai, CCPA ir vėliau patobulintame CPRA, nėra nustatyti absoliutūs neskelbtinos asmeninės informacijos draudimai. Vietoj to, CPRA plačiai apibrėžia "jautrią asmeninę informaciją" įvardindama jog ji apima vyriausybės identifikatorius, tikslią geografinę vietą, rasinę ar etninę kilmę, biometrinius ir sveikatos duomenis - ir suteikia vartotojams teisę apriboti jos naudojimą įgyvendinant savo teises ir konkrečius pranešimo reikalavimus (Hogan Lovells, 2021). Tačiau CPRA trūksta niuansuotos teisinės ribos, lygiavertės BDAR 9 straipsniui. Jame nereikalaujama konkretaus teisinio pagrindo tvarkyti jautrią asmeninę informaciją, išskyrus BPDI siunčiamus bendro pobūdžio pranešimus ir komplikuotą galimybę pasinaudoti atsisakymo mechanizmu. Pagal šį modelį daroma prielaida, kad naudotojas veikia ir yra sąmoningas, o tai gali būti neveiksminga itin techniškoje ar neskaidrioje BPDI aplinkoje. Mokslininkai teigia, kad dėl jautrios asmeninės informacijos atsisakymo pobūdžio asmenims užkraunama neproporcingai didelė našta apsisaugoti patiems, užuot reikalavus sisteminių apsaugos priemonių (Hoofnagle et al., 2018).

Ypač sudėtinga kategorija BPDI kontekste yra išvestiniai duomenys - informacija, gauta iš kitų šaltinių pasitelkiant LLM sistemų algoritmus. Iš netiesioginių duomenų, pavyzdžiui, kalbos vartojimo, naršymo istorijos ar socialinių ryšių, DI sistemos gali nustatyti tokius jautrius požymius kaip seksualinė orientacija, politinės pažiūros ar psichinės sveikatos būklė. Svarbu išskirti, kad BDAR nedaro skirtumo tarp surinktų ir išvestinių asmens duomenų, jei juos galima susieti su pavieniu duomenų subjektu, kadangi kiekvienam duomeniui užtikrinami saugomo reikalavimai. Tuo galima įsitikinti pažvelgus į BDAR 5 ir 22 straipsnius, kuriuose pabrėžiamas sąžiningumas, tikslo apribojimas ir draudimas priimti svarbius sprendimus vien tik remiantis automatizuotomis priemonėmis be žmogaus priežiūros (Wachter, Mittelstadt, 2018). Priešingai, tiek CCPA, tiek ir CPRA pripažįstama, kad egzistuoja išvestiniai duomenys, tačiau užtikrinama palyginti silpna apsauga. Pagal CPRA išvestinės charakteristikos pagal jautrius asmens duomenis laikomos tik tada, kai jos gaunamos iš duomenų subjekto veiklos ir naudojamos profiliavimui. Tačiau profiliavimo *per se* nedraudžiama, taip pat įstatymu neribojamas automatizuotas sprendimų priėmimas, išskyrus atvejus, kai jis aiškiai reglamentuojamas kituose sektoriniuose įstatymuose. Kalifornijos generalinė prokuratūra patikslino, kad įmonės privalo tik atskleisti, ar jos daro išvadas apie duomenis, ir pasiūlyti ribotas vartotojų teisių gynimo priemones, išskyrus atvejus, kai duomenys parduodami arba jais dalijamasi (Calawyers.org, 2024). Tokia fragmentiška apsauga kontrastuoja su BDAR struktūrizuota sistema, kurioje numatytas ne tik skaidrumas, bet ir prasmingas žmogaus įsikišimas profiliavimo kontekstuose.

Pseudoniminiai duomenys suteikia dar vieną teisinio sudėtingumo lygmenį. Pagal BDAR pseudoniminiai duomenys, tai yra duomenys, kurių negalima priskirti asmeniui be papildomos, atskirai saugomos informacijos, tačiau vis tiek yra laikomi asmens duomenimis ir turi būti atitinkamai saugomi. Nors pseudoniminiai duomenys yra skatinami kaip saugumo priemonė, jis neatleidžia duomenų valdytojų nuo pareigų. Tai ypač aktualu BPDI mokymuose, kur pseudoniminiai duomenys dažnai naudojami siekiant išvengti tiesioginio identifikavimo. Atitinkamai BDAR reikalaujama imtis griežtų organizacinių ir techninių priemonių, pavyzdžiui, diferencijuoto privatumo arba federacinio mokymosi, kad būtų sumažinta pakartotinio identifikavimo rizika. Pagal CPRA pseudoniminiai duomenys taip pat yra apibrėžiami, tačiau skirtingai nei ES atžvilgiu, traktuojami lanksčiau. Įmonės gali būti atleistos nuo atitikties prievolių, jei pseudoniminiai duomenys naudojami tik vidaus mokslinių tyrimų ar veiklos tikslais ir nebandoma pakartotinai nustatyti tapatybės. Tačiau nėra prievolės verslo subjektams, teikiantiems BPDI paslaugas, įgyvendinti

konkrečias privatumo išsaugojimo priemones, o pseudoniminiams duomenims netaikomos visos vartotojų teisės pagal CPRA, nebent jie pakartotinai gali būti susiejami su asmeniu, kurio tapatybę yra įmanoma nustatyta. Kritikai teigia, kad šia spraga galima pasinaudoti dirbtinio intelekto kūrimo aplinkoje, ypač mokantis pagal elgsenos ar biometrinių duomenų rinkinius.

Anoniminiai duomenys – yra laikoma duomenims, iš kurių negrįžtamai pašalinti asmens identifikatoriai - teoriškai netaikomi nei BDAR, nei CCPA. Tačiau praktiškai tikrąjį anonimiškumą pasiekti yra sunku. BDAR šiuo atžvilgiu nustatyta aukšta riba, tai yra duomenys negali būti identifikuoti pakartotinai kitos ar trečiosios šalies, naudojant bet kokias priemones, kurios "pagrįstai gali būti panaudotos identifikacijai". BPDI kontekste šį standartą atitikti dar sunkiau, nes dideli kalbos modeliai gali tarptautiniu mastu taikyti statistinius duomenų, pagal kuriuos jie buvo apmokyti, pėdsakus, todėl atsiranda pakartotinio identifikavimo arba netyčinio įsiminimo galimybė. Todėl ES reguliavimo institucijos pasisako už dinamiškus, į kontekstą orientuotus anoniminių duomenų vertimo metodus, o ne už tai, kad anoniminiai duomenys būtų laikomi pastovia būkle (CIPL, 2024). Priešingai, CPRA pateikta anoniminių duomenų apibrėžtis yra platesnė ir mažiau techniškai apibrėžta. Joje tik reikalaujama, kad duomenų nebūtų galima pagrįstai identifikuoti ar susieti su konkrečiu vartotoju, ar namų ūkiu, nenurodant techninių priemonių, kurių reikia tokiam rezultatui pasiekti. Dėl to bendrovėms paliekama galimybė skelbti duomenis "anonimiškais" be griežto anoniminių duomenų vertimo taikymo, ypač aplinkoje, susijusioje su didžiuliais, integruotais duomenų rinkiniais, tokiais kaip BPDI mokomieji korpusai. Todėl CPRA gali leisti išvengti duomenų reguliavimo, nepaisant nuolatinės pakartotinio tapatybės nustatymo ir žalos rizikos.

Apibendrinant galima teigti, kad nors ir BDAR kaip ir CPRA siekiama apibrėžti asmens duomenų kategorijas ir užtikrinti naudotojų apsaugą, jų taikymo sritis, teisinis griežtumas ir vykdymo užtikrinimo logika labai skiriasi. BDAR pirmenybė teikiama sisteminei atskaitomybei, reikalaujant pagrįsti duomenų tvarkymą kiekviename etape ir atsargiai traktuojant net išvestinius ar pseudoniminius duomenis. Nors CPRA yra svarus žingsnis į priekį JAV duomenų privatumo teisėje, jis vis dar daugiausia remiasi vartotojų veiksmais ir neapima viso duomenų gyvavimo ciklo, t. y. nuo informacijos surinkimo iki jos paviešinimo, dirbtinio intelekto ekosistemose. Plėtojantis BPDI, asmens duomenų - ypač išvestinių, pseudoniminių ir neskelbtinų duomenų - teisinis traktavimas turės atspindėti vis labiau nelinijinį ir besiformuojantį mašininio mokymosi procesų pobūdį.

Norint užtikrinti, kad privatumo apsauga išliktų prasminga ir įgyvendinama šioje naujoje paradigmoje, reikės teisėkūros reformos ir reguliavimo derinimo.

1.4. ES IR JAV TEISINIO REGULIAVIMO SKIRTUMAI IR PANAŠUMAI, ESMINIAI IŠŠŪKIAI SIEKIANT VIENINGO POŽIŪRIO Į BENDROSIOS PASKIRTIES DIRBTINĮ INTELEKTĄ

ES ir JAV teisinės tradicijos skirtumai ir filosofijų išsiskyrimas dėl DI reguliavimo yra vienas sudėtingiausių teisinių iššūkių valdant BPDI. Šie skirtumai yra giliai įsišakniję atitinkamose teisinėse tradicijose ir socialiniame bei politiniame kontekste. ES pirmenybė teikiama pagrindinėms teisėms, ypač duomenų apsaugai ir žmogaus orumui, o JAV sistemoje pirmenybė paprastai teikiama rinkos efektyvumui, inovacijoms ir minimaliam valstybės įsikišimui. Kadangi BPDI sistemos vis labiau lemia viešųjų ir privačių sprendimų priėmimą tiek komerciniame, tiek ir privačiame lygmenyje bei siekiant išsamiai atskleisti temą yra labai svarbu suprasti šių dviejų jurisdikcijų reguliavimo skirtumus. Todėl šis skyrius pradedamas skirtingų teisinių tradicijų apžvalga, bendrinio požiūrio kampo atskleidimu, o toliau pereinama prie abiejų jurisdikcijų požiūrio į verslą ir inovacijas, taip pat kokiu mastu asmeniui, kaip duomenų subjektui, teikiama pirmenybė prieš kitas vertybes.

1.4.1. BENDRINIS POŽIŪRIS Į VERSLĄ, JO PLĖTROS GALIMYBES

BPDI atsiradimas sukėlė intensyvų teisinį ir politinį diskursą dėl vyriausybių vaidmens reguliuojant dirbtinio intelekto inovacijas. Pagrindinė šių diskusijų tema - kaip sukurti tvarią aplinką technologinei pažangai, nepažeidžiant privatumo, atsakomybės ir etikos standartų. Lyginant abidvi teisines sistemas, gali įžvelgti skirtingų kontrastų suderinamumą - ES remiasi aktyvia teisine intervencija, grindžiama žmogaus teisėmis ir rizikos vertinimu, o JAV priešingai vadovaujasi į rinką orientuota ir į inovacijas nukreiptu požiūriu. Šie išsiskiriantys požiūriai lemia labai priešingą reguliavimo aplinką, kuri daro tiesioginę įtaką verslo galimybėms ir padeda formuoti atitikties lūkesčius BPDI kūrėjams.

2024 m. ES oficialiai priimtame DI akte DI sistemos skirstomos į rizikos lygius, o kiekvienai kategorijai priskiriami konkretūs įpareigojimai. Nors BPDI sistemos paprastai nelaikomos "didelės rizikos" sistemomis, nebent jos atlieka svarbiausias visuomenės funkcijas, pavyzdžiui, biometrinio identifikavimo ar švietimo, bendrosios paskirties AI

modeliams, pavyzdžiui, dideliems kalbų modeliams, vis dėlto taikomi kompleksiniai įpareigojimai. Tarp jų patenka privalomas AI sukurto turinio ženklinimas, mechanizmų, užkertančių kelią neteisėtiems rezultatams, kūrimas ir mokymui naudotos autorių teisių saugomos medžiagos santraukų atskleidimas (Veale, Borgesius, 2021). Reglamentas įkūnija visapusišką *ex ante* požiūrį, pirmenybę teikiant skaidrumui, dokumentavimui ir atskaitomybei, kad kaip įmanoma geriau būtų apsaugotos pagrindinės duomenų subjekto teisės.

Duomenų apsaugos sritį analizuojantys mokslininkai pabrėžia, kad šis modelis atspindi gilesnį normatyvinį įsipareigojimą dėl duomenų suverenumo ir algoritmų skaidrumo (Brkan, 2019). Nustatydama apribojimus privataus sektoriaus autonomijai diegiant BPDI, ES bando užtikrinti, kad technologinė plėtra atitiktų demokratines vertybes. Įpareigojimas saugoti mokymo duomenų įrašus, užtikrinti algoritmų sąžiningumą ir pateikti išankstinius atitikties vertinimus iliustruoja platesnį judėjimą link to, ką mokslininkai vadina "algoritminiu konstitucionalizmu". Šiai vizijai pritaria ir Floridi et al. (2018), kurie teigia, kad į dirbtinio intelekto reguliavimą turi būti įtraukta "projektinė etika" kaip priemonė visuomenės interesams apsaugoti.

Tačiau šis griežtas reglamentavimas neapsieina be prieštaravimų. Pramonės atstovai tvirtina, kad didelės reikalavimų laikymosi išlaidos gali trukdyti Europos konkurencingumui kuriant dirbtinį intelektą pasaulyje, ypač pradedančiosioms įmonėms ir mažoms bei vidutinėms įmonėms. Europos startuolių tinklas (2023 m.) pažymi, kad biurokratinės išlaidos, susijusios su atitikties vertinimu, gali sulėtinti Europos inovacijų pateikimo rinkai laiką. Reaguodama į tai, Europos Komisija paskelbė smėlio dėžės iniciatyvas ir finansavimo mechanizmus, skirtus atsakingoms inovacijoms, nukreiptoms ypač mažosioms ir vidutinėms įmonėms skatinti, atsižvelgiant jog jos veikia esant ribotiems ištekliams.

Tuo tarpu JAV nėra vieningos teisinės sistemos, skirtos dirbtinio intelekto reguliavimui, o tai atspindi istoriškai susiklosčiusį „palik gyvenimui savaime viską sudėlioti“ požiūrį, pagal kurį daugiausia dėmesio skiriama inovacijoms ir rinkos plėtrai. Nors Bideno administracijos 2023 m. vykdomajame įsakyme Nr. 14110 nustatyti patikimo dirbtinio intelekto principai, įskaitant privatumo, pilietinių teisių ir darbuotojų apsaugos klausimus, jam trūko privalomos teisinės galios. Jo atšaukimas 2025 m. pradžioje, kai jį atšaukė kita administracija, dar kartą iliustruoja JAV reguliavimo politikos nepastovumą. Nesant centrinės teisinės struktūros, teisės aktų vykdymas išlieka išskaidytas tarp federalinių agentūrų ir valstijų vyriausybių.

Valstijų lygmens veiksmai iš dalies užpildo reguliavimo vakuumą. Pavyzdžiui, Kalifornijoje priimtame SB 1047 siūlomi griežti BPDI modelių saugos ir valdymo standartai. Nors galiausiai jis buvo vetuotas dėl susirūpinimo dėl jo ribotumo, šis įstatymo projektas parodė didėjantį valstijų norą eksperimentuoti su dirbtinio intelekto valdymo sistemomis. Vis dėlto federalinio suderinimo trūkumas sukuria fragmentišką reglamentavimo aplinką, kuri apsunkina keliose jurisdikcijose veikiančių subjektų atitiktį įstatymams (Nix, Bizarro, 2020). Pramonės iniciatyvos ir etinės gairės, pavyzdžiui, Nacionalinio standartų ir technologijų instituto DI rizikos valdymo sistema, tarnauja kaip savanoriški atsvaros taškai, tačiau tai tik rekomendacinio pobūdžio informacija, kurios laikymasis ar bent atsižvelgimas į ją yra paremtas tik geromis intencijomis.

Lyginant šiuos skirtingus požiūrius, galima teigti, kad jie grindžiami iš esmės skirtingomis teisės filosofijomis. ES reguliavimą suvokia kaip priemonę technologinėse sistemose įtvirtinti etines ir teisines normas - modelį, kurį teisės teoretikai, pavyzdžiui, Floridi et al. (2018), vadina "etika pagal dizainą". Ir priešingai, JAV taikomas reaktyvusis modelis, pagal kurį reguliavimas dažnai atsiranda dėl rinkos nepakankamumo ar visuomenės spaudimo, o ne dėl išankstinių apribojimų, pasikliaujant teisminiais ginčais ir savi reguliaciniais kodeksais. Kaip teigia Crawfordas ir Paglenas (2021), ES "formuoja" dirbtinį intelektą per teisėtumą ir įstatymų leidybą, o JAV "reaguoja" per teismus ir sutartis. Tokie įvairialypiai skirtumai sukuria BPDI kūrėjams praktinių iššūkių, kurių būtų galima išvengti bandant ieškoti vieningo požiūrio. Tačiau ES taisyklėse reikalaujama, kad įmonės dokumentuotų mokymo duomenų rinkinius, skelbtų technines santraukas ir žymėtų, kad rezultatai sukurti pasitelkiant DI. JAV tokia praktika skatinama per etikos sistemas, tačiau nėra privaloma, todėl verslas dažniausiu atveju renkasi neišlaidauti bei nesivarginti antraeiliais klausimais. Tai gali lemti nevienodą skaidrumą ir atskaitomybę, priklausomai nuo jurisdikcijos. Be to, ekstra teritorinis ES reguliavimo srities taikymas verčia net ne ES kūrėjus pritaikyti savo sistemas, kad jos atitiktų Europos standartus, jei jie veikia jos skaitmeninėje rinkoje.

Apibendrinant galima daryti išvadą, kad ES modelis yra aukšto reguliavimo ir aukšto pasitikėjimo aplinka, kuria siekiama kurti atsakingas dirbtinio intelekto ekosistemas, o JAV ir toliau palaiko inovacijoms palankias, bet fragmentiškas struktūras. Šie skirtumai atspindi ne tik politinius sprendimus, bet ir gilesnes visuomenės vertybes: ES žmogaus orumas ir duomenų apsauga yra konstituciniai principai, o JAV dominuoja verslo laisvė ir minimalus valstybės įsikišimas. Kadangi BPDI sistemos tampa vis galingesnės ir vis labiau paplitusios, tarptautinio koordinavimo poreikis tampa neatidėliotinas, tačiau kyla esminis

klausimas kaip iš esmės priešingos sistemos atras unifikuotą poziciją. Konvergencija per dvišales ar daugiašales sistemas gali būti būdas suderinti standartus ir užtikrinti subalansuotą valdymą, kuriuo remiamos ir inovacijos, ir pagrindinės teisės.

1.4.2. (NE)PRIORETIZAVIMAS ASMENS, KAIP DUOMENŲ SUBJEKTO

Asmens, kaip duomenų subjekto, (ne)prioriteto suteikimas BPDI reguliavimo sistemose atskleidžia esminius filosofinius, institucinės sandaros ir teisinius skirtumus tarp ES ir JAV. ES remiasi teisėmis grindžiamu požiūriu į duomenų apsaugą, kuris įtvirtintas Europos Sąjungos pagrindinių teisių chartijoje. Šis požiūris pabrėžia žmogaus orumo ir autonomijos svarbą kaip skaitmeninio valdymo pagrindą. Reguliacinė orientacija siekia užtikrinti, kad net ir sudėtingų bei neskaidrių dirbtinio intelekto sistemų kontekste asmenys išlaikytų teisę kontroliuoti savo duomenis.

Teisės mokslininkai, tokie kaip Brkan (2019), pažymi, kad pagal BDAR struktūrą asmuo nebėra tik pasyvus teisinės apsaugos objektas – jis apibrėžiamas kaip aktyvus ir įgalintas subjektas, turintis aiškias teises veikti. Tokios teisės kaip prieiga prie duomenų, jų ištaisymas, ištrynimas, duomenų perkėlimas ar teisė nesutikti su automatizuotu sprendimų priėmimu nėra tik deklaratyvios – jos yra privalomos ir turi būti užtikrinamos tiek viešojo, tiek privataus sektoriaus veikėjų. BPDI kūrėjai turi atsižvelgti į šias teises ir įtraukti jas į savo sistemų technologinį dizainą. Šiuos principus papildo priežiūros institucijų, tokių kaip Prancūzijos duomenų apsaugos institucija (toliau „**CNIL**“), gairės. CNIL (2023) atkreipė dėmesį į „juodosios dėžės“ modelių neskaidrumą ir pabrėžė skaidrumo, paaiškinamumo bei žmogiškosios priežiūros būtinybę. Tokie instituciniai išaiškinimai prisideda prie reguliacinės aplinkos stiprinimo ir sustiprina asmens teisių užtikrinimą BPDI kontekste.

Tuo tarpu JAV duomenų apsauga nėra laikoma pamatine teise ir nėra reguliuojama vieningu teisės aktu, prilygstančiu BDAR. JAV modelyje, atsižvelgiant į jo istorinę raidą ir dabartinę trajektoriją, privatumas traktuojamas kaip vartotojo teisė, o ne kaip esminė žmogaus teisė. Nors tam tikri įstatymai, pavyzdžiui, CCPA ir jį papildęs CPRA, numato vartotojams atsisakymo mechanizmus, jie nėra tokie išsamūs nei struktūriniu, nei procedūriniu požiūriu kaip ES sistemoje. Gasser ir Almeida (2017) kritikavo šį JAV požiūrį kaip reaktyvų ir rinkos principais paremtą modelį, kuris dažnai lemia „sprendimo priėmimo nuovargį“ bei neefektyvius vykdymo užtikrinimo mechanizmus. Praktiškai tai, kad JAV reguliavimo aplinkoje asmeniui neteikiamas prioritetas, pasireiškia ribota priežiūra, savanorišku reikalavimų laikymusi ir fragmentišku teisiniu vykdymu. Asmenys turi

orientuotis ilgoje privatumo politikoje, neaiškiose sutikimo nuorodose ir neadekvačiuose teisių gynimo mechanizmuose. Be to, JAV reikalavimas įrodyti žalą kaip išankstinę teisinių veiksmų sąlygą dar labiau susilpnina praktinį asmens teisių įgyvendinimą. Kuner ir kt. (2020) pažymi, kad ši riba trukdo aktyviam valdymui ir riboja neturtinės žalos, pavyzdžiui, DI algoritmo šališkumo atveju ar esant netinkamam duomenų naudojimui, atlyginimą. BPDI kontekste kai duomenų subjektai dažnai net nežino, kad jų duomenys buvo tvarkomi, tokios vykdymo užtikrinimo kliūtys kenkia teoriniam teisių pripažinimui. Priešingai, ES teisėje įrodinėjimo ir pagrindimo našta tenka duomenų valdytojui, todėl asmenų ir institucijų galios santykiai yra simetriškesni.

Floridi ir kt. (2018) pabrėžia, kad etiškoje dirbtinio intelekto ekosistemoje turi būti orientuojamasi į asmenį, integruojant ne tik teisinius, bet ir normatyvinius principus, kurie neapsiriboja tik atitiktimi. Šis požiūris atitinka BDAR etosą, tačiau Amerikos teisėkūros debatuose jo iš esmės nėra. Be sistemos, kurioje struktūriškai pirmenybė teikiama asmeniui, BPDI gali sustiprinti esamą nelygybę, pagilinti priežiūros asimetriją ir sudaryti sąlygas neatsakingam algoritmais paremtam subjekto valdymui. Galima teigti, kad ES įtvirtina asmenį kaip teisinę ir etinę BPDI valdymo atramą, užtikrinant apsaugą per įgyvendinamas teises ir institucinius mechanizmus. JAV, nors ir pažengusios duomenų privatumo supratimo srityje, toliau į asmenį žiūri kaip į vieną iš daugelio suinteresuotųjų šalių, pavaldžią ekonominiams ir technologiniams prioritetams. Dėl šių struktūrinių skirtumų BPDI kūrėjams kyla ne tik atitikties reikalavimų laikymosi problemų, bet ir iš esmės skiriasi ateities skaitmeninės visuomenės vizijos.

2. DUOMENŲ TVARKYMO TEISĖTUMO IR ATSAKOMYBĖS PROBLEMOS BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO RĖŽIUOSE

BPDI sistemų atsiradimas iš esmės pakeitė asmens duomenų rinkimo, tvarkymo ir naudojimo būdus. Šios sistemos, kurios veikia mokydamosi iš didžiulių, dažnai nestruktūrizuotų duomenų rinkinių, kelia sudėtingų klausimų dėl duomenų naudojimo teisėtumo, jų rinkimo tikslo ir atsakingų subjektų nustatymo. Šio sudėtingumo esmė - esminis teisinis klausimas: ar esami duomenų apsaugos principai gali tinkamai reglamentuoti technologijas, kurių architektūra ir rezultatai laikui bėgant vystosi autonomiškai? Atsakymas negalėtų būti paprastas, nepaisant to, kad BDAR suformuluoti tokie pamatiniai principai kaip tikslo apribojimas, duomenų kiekio mažinimas ir

atskaitomybė. Tačiau, kaip pastebi Kuner ir kt. (2020), šių principų taikymas BPDI toli gražu nėra paprastas, nes šios sistemos retai kuriamos remiantis aiškiai apibrėžtu, vieninteliu tikslu ir dažnai keičia duomenų paskirtį naudodamos abstrakcijos ir išvadų generavimo sluoksnius. Panašiai Zaleskis (2019) pabrėžia, kad tradicinis duomenų subjekto vaidmuo ir jo teisės į skaidrumą ir ištrynimą tampa labai pažeidžiamos, kai dirbtinio intelekto sistemos slepia asmens duomenų kilmę ir transformaciją. Tai ypač problemiška, kai išvestinių išvadų - pavyzdžiui, profilių, elgesio modelių ar susintetintos kalbos - negalima lengvai atsekti iki pirminių duomenų įvesties, taip susilpninant teisių įgyvendinamumą ir didinant teisinį netikrumą.

Padėtį dar labiau apsunkina atskaitomybės klausimas: paskirstytas ir daugiasluoksnis BPDI sistemų pobūdis dažnai apima daug dalyvių, įskaitant kūrėjus, duomenų teikėjus, sistemų adaptuotojus ir galutinius naudotojus, kurių atsakomybė pagal esamas teisines sistemas nėra aiškiai apibrėžta. BDAR bandoma apibrėžti duomenų valdytojų ir duomenų tvarkytojų pareigas, tačiau, kaip pastebi Kuner ir kt. (2020), dinamiškose, savaime besimokančiose sistemose riba tarp šių vaidmenų tampa neaiški. Tuo tarpu JAV duomenų apsaugos įstatymuose, pavyzdžiui, CCPA ir CPRA, numatyta fragmentiška ir ne tokia išsami apsauga, nes juose nėra Europos teisėje įtvirtintų patikimų atskaitomybės mechanizmų. Todėl šiame skyriuje siekiama išnagrinėti šiuos daugialypius teisėtumo ir atskaitomybės klausimus, pradedant nuo 2.1 skirsnyje pateikto pagrindinio nesutarimo tarp duomenų rinkimo praktikos ir tikslo apribojimo principo. Toliau bus vertinami pakartotinio tapatybės nustatymo, algoritmais paremtų rezultatų neskaidrumo ir platesnio masto sprendimų priėmimo delegavimo ne žmogiškiesiems subjektams padariniai. Apibūdinant šiuos iššūkius ES ir JAV reguliavimo srityse, šiame skyriuje siekiama įvertinti, ar dabartinės teisinės priemonės yra pritaikytos patenkinti sparčiai besivystančios BPDI ekosistemos poreikius, ir, jei reikia, pasiūlyti interpretacinius ar normatyvinius patobulinimus šioms atsirandančioms spragoms pašalinti.

2.1. KONFLIKTAI TARP DUOMENŲ RINKIMO IR TIKSLO APRIBOJIMO PRINCIPŲ

Vis plačiau diegiant BPDI sistemas kyla esminių prieštaravimų tarp inovacijų užmojo ir teisinės pareigos saugoti asmens duomenis, ypač atsižvelgiant į BDAR 5 straipsnio 1 dalies b punkte numatytą tikslo apribojimo principą. Šioje nuostatoje nustatyta, kad asmens duomenys turi būti renkami konkrečiais, aiškiai apibrėžtais ir teisėtais tikslais ir neturi būti toliau tvarkomi su tais tikslais nesuderinamu būdu (Kuner ir kt., 2020). Tačiau BPDI dažnai nukrypsta nuo šio principo, nes remiasi masiniu, apibendrintu duomenų rinkimu ir nėra aiškaus duomenų naudojimo ir nurodytų tikslų suderinimo. Duomenys, naudojami tokiems modeliams, kaip OpenAI GPT-4 arba Google Gemini, mokyti, paprastai gaunami iš didelio masto interneto duomenų nuskaitymo operacijų. Šiomis operacijomis renkama informacija iš įvairių viešų šaltinių - tinklaraščių, forumų ir socialinės žiniasklaidos, kuriuose dažnai yra asmens duomenų, neskirtų antriniam naudojimui. Europos duomenų apsaugos valdyba (EDPB, 2020) pakartojo, kad viešas prieinamumas neatleidžia duomenų valdytojo bei tvarkytojo nuo BDAR taikymo srities, ypač tais atvejais, kai duomenų subjekto lūkesčiai nebuvo profiliuoti ar pakartotinai naudoti nesusijusiems mašininio mokymosi tikslams.

Daugelyje tyrimų pabrėžiama, kad asmens duomenų buvimas BPDI mokymo rinkiniuose kelia rimtų atitikties problemų. Rocher, Hendrickx ir Shmatikov (2019 m.) parodė, kad panaikinus duomenų tapatybę galima iš naujo identifikuoti naudojant mašininio mokymosi išvadas ir pagalbinius duomenų rinkinius. Dar labiau komplikuojant situaciją, Carlini ir kiti (2023) pademonstravo "duomenų nutekėjimą" - reiškinį, kai BPDI sistemos netyčia atkuria neskelbtinus arba privačius fragmentus iš savo mokymo duomenų rinkinių. Tokiai rizikai sumažinti buvo pasiūlytos tokios techninės strategijos kaip diferencinis privatumas, „homomorfinis“ šifravimas ir federacinis mokymasis. Tačiau Veale ir Binns (2017) pastebi, kad šie metodai, nors konceptualiai yra patikimi, dažnai susiduria su įgyvendinimo kliūtimis dėl išlaidų, techninio sudėtingumo arba pramonės standartų trūkumo. Tai mažina jų naudingumą siekiant apsaugoti tikslo apribojimo principą, ypač kai jie taikomi neskaidrioms komercinėms BPDI architektūroms.

BDAR duomenų valdytojams nustatytos griežtos pareigos dokumentuoti ir apriboti duomenų tvarkymo tikslus. 29 straipsnio darbo grupė (2013 m.) pabrėžė, kad bet kokiam antriniam naudojimui turi būti atliekamas suderinamumo testas, atsižvelgiant į kontekstą, duomenų pobūdį ir duomenų subjekto lūkesčius. Tokie testai retai atliekami BPDI taikomosiose programose, kuriose didžiuliai duomenų rinkiniai pakartotinai naudojami

daugelyje sričių. Kūrėjai retai seka metaduomenis arba tvarko dokumentus, kurių pakanka BDAR skaidrumo ir atskaitomybės reikalavimams įvykdyti. Priešingai, JAV požiūriui, kuriam būdingi CCPA ir CPRA, nėra tikslo apribojimui lygiaverčio principo. Vietoj to JAV remiasi "pranešimo ir pasirinkimo" paradigma, kurią mokslininkai, pavyzdžiui, Schwartz ir Solove (2014), kritikavo kaip neveiksmingą šiuolaikinėse skaitmeninėse ekosistemose, kuriose naudotojus užvaldo informacijos asimetrija ir prievartiniai sutikimo mechanizmai.

Mokslinėje literatūroje įspėjama apie platesnį nekontroliuojamo GenAI kūrimo poveikį visuomenei. Zuboffas (2019) aprašo "priežiūros kapitalizmo" atsiradimą, kai asmeniniai duomenys tampa preke ir naudojami be aiškaus sutikimo, o tai kelia iššūkį demokratinei technologijų kontrolei. Tisné (2020) panašiai teigia, kad struktūrinės atskaitomybės nebuvimas skatina duomenų praktiką, kuri pabrėžia asmens autonomiją. Siekdami spręsti šias grėsmes, Raji et al. (2020) ir Morley et al. (2021) pasisako už algoritmų poveikio vertinimą, duomenų atsekamumo auditą ir dokumentavimo priemones, pavyzdžiui, duomenų rinkinių duomenų lapus ir modelių korteles (Gebru et al., 2018). Šie mechanizmai gali padidinti skaidrumą ir vėl susieti modelių kūrimą su pradiniais teisiniais ir etiniais apribojimais.

ES AI aktas yra žingsnis siekiant suderinti AI valdymą su BDAR principais, visų pirma taikant rizika grindžiamą klasifikavimą ir privalomą atitikties vertinimą. Gellert (2023) pažymi, kad nesant teisinių režimų sąveikos, gali atsirasti prieštaringų pareigų, o tai gali supainioti atitikties užtikrinimo pastangas. BDAR 6 straipsnio 4 dalyje numatyti antrinio naudojimo vertinimo kriterijai, įskaitant tikslų suderinamumą ir poveikį duomenų subjektui. Tačiau dėl BPDI "juodosios dėžės" pobūdžio ir kintančių duomenų srautų šiuos vertinimus sunku atlikti praktiškai. Mantelero (2018) įspėja, kad adaptyviose dirbtinio intelekto sistemose išlieka didelė "funkcinio šliaužimo" - laipsniško duomenų naudojimo išplėtimo už pirminio tikslo ribų - rizika. Nesant aiškių dokumentų ir sutikimo, net ir techniškai nuasmeninti duomenys gali būti atskleisti asmeniškai.

Apibendrinant galima daryti išvadą, kad BPDI duomenų praktikos ir BDAR tikslo apribojimo principo prieštaravimas išryškina gilesnį šiuolaikinės technologinės praktikos ir tradicinių teisinių apsaugos priemonių nesuderinamumą. Šiam atotrūkiui įveikti reikia suderinti teisines sistemas, įdiegti technines apsaugos priemones ir sustiprinti institucinę priežiūrą. Teisinė reforma, technologinio projektavimo principai ir tarpsektorinis dialogas turi būti derinami siekiant užtikrinti, kad duomenimis grindžiamos inovacijos nesumažintų teisių, kurias siekiama stiprinti. BPDI ateitį turi lemti ne tik technologiniai pajėgumai, bet ir principinis įsipareigojimas užtikrinti žmogaus orumą ir duomenų apsaugą.

2.2. ASMENS DUOMENŲ IDENTIFIKAVIMO RIZIKA NET IR ANONIMINIŲ AR PSEUDONIMINIŲ DUOMENŲ ATVEJAIS

Bendrosios paskirties dirbtinio intelekto (BPDI) eroje vis dažniau tikrinamas anoniminis ir pseudoniminis, kaip duomenų apsaugos mechanizmų, veiksmingumas. Nors abi sąvokos padeda sumažinti riziką duomenų subjektams, teisinės ir techninės realijos rodo esminius apribojimus. Pagal ES BDAR pseudoniminiai duomenys, kai identifikuojami elementai pakeičiami dirbtiniais identifikatoriais vis tiek laikomi asmens duomenimis, nes išlieka galimybė juos pakartotinai susieti (BDAR, 2 str. 4(5)). Ir priešingai, anoniminiai duomenis norint gauti, reikia negrįžtamai pakeisti duomenis iki būsenos, kai asmenų tapatybės nebegali nustatyti joks subjektas, naudodamasis bet kokiomis pagrįstai prieinamomis priemonėmis (BDAR, 26 konstatuojamoji dalis). Tačiau tobulėjant BPDI sistemoms ir jas palaikančioms skaičiavimo galimybėms, tai, kas anksčiau buvo laikoma nuasmenintais duomenimis, gali būti nebeatpažįstama iš naujo.

Siūlomas ES DI aktas grindžiamas šia sistema, visų pirma rizika pagrįstu klasifikavimo modeliu. Įstatymu įpareigojama atlikti griežtą didelės rizikos dirbtinio intelekto sistemų, įskaitant tas, kuriose naudojami asmens arba netiesiogiai susieti duomenys, rizikos vertinimą (Europos Komisija, 2021 m.). Naujausioje literatūroje (Gellert, 2023; Veale et al., 2021) pažymima, kad net anoniminiai duomenų rinkiniai, naudojami mokant dirbtinio intelekto modelius, gali kelti Vidutinę riziką, ypač kai įmanoma atlikti duomenų „trianguliaciją“ arba kryžminę nuorodą su pagalbiniais duomenų rinkiniais. Taigi, BPDI sistemos, kuriose naudojami didžiuliai, nevienalyčiai duomenų fondai, negali užtikrintai teigti, kad jos atitinka reikalavimus vien dėl anoniminių duomenų vertimo metodo. Be to, tokios reguliavimo institucijos kaip EDPB (2020) įspėja, kad anoniminių duomenų vertimas neturėtų būti vienkartinis procesas, o turi būti nuolat vertinamas atsižvelgiant į besivystančias pakartotinio identifikavimo galimybes.

Jungtinėse Amerikos Valstijose Kalifornijos vartotojų privatumo įstatyme (CCPA) ir Kalifornijos privatumo teisių įstatyme (CPRA) taikoma ne tokia griežta apibrėžtis. De identifikuotų duomenų neturi būti galima susieti su konkrečiu asmeniu, tačiau tokio nesusiejamojo užtikrinimo standartai iš esmės nėra apibrėžti (CCPA §1798.140(h); CPPA, 2022 m.). CPRA nustatyta daugiau atskaitomybės, reikalaujant, kad įmonės sutartimis įpareigotų de identifikuotų duomenų gavėjus užkirsti kelią pakartotiniam identifikavimui. Tačiau teisės mokslininkai ir duomenų apsaugos ekspertai išreiškė susirūpinimą, kad tokiuose įstatymuose, kaip CPRA, nustatytos apsaugos priemonės, nors ir tariamai tvirtos,

dažnai priklauso nuo vidinės organizacijos politikos, o ne nuo aiškiai apibrėžtų ir techniškai įgyvendinamų standartų. Be to, neseniai atlikti JAV įsikūrusių BPDI kūrėjų tyrimai atskleidė duomenų tapatybės panaikinimo praktikos nenuoseklumą, ypač mokant LLM pagal viešai prieinamus, tačiau potencialiai neskelbtinus tekstinius duomenis (Hovy, Spruit, 2023).

Naujausi tyrimai rodo, kad anonimiškumas BPDI srityje yra lengvai pažeidžiamas ir suteikiama apsauga yra greičiau iliuzija nei efektyvus būdas apsisaugoti. Carlini ir kt. (2023) empiriškai įrodė, kad difuzijos ir transformacijos modeliai gali atkurti mokymo duomenis - įskaitant vardus, el. pašto adresus ir net telefono numerius - kai tikslingomis informacijos įvestimis yra to siekiama. Ši informacijos nutekėjimo rizika tiesiogiai kvestionuoja prielaidą, kad anoniminių ir šifruotų duomenų rinkiniai negali lemti asmens identifikavimo. Be to, Liu ir kt. (2024) atliktame DI apžvalgos tyrime pabrėžiama, kad BPDI modeliams mokyti paprastai naudojami LLM rinkiniai, dažnai sudaromi iš interneto platybėse surandamo ir apdorojamo didžiulio kiekio teksto. Apžvalgoje pabrėžiama, kad net ir taikant šifravimo metodus, dėl didelių LLM rinkinių matmenų ir sistemų sudėtingumo gali kilti reali rizika privatumui, ypač kai modeliai pakartotinai tikslinami pagal konkrečios srities duomenis. Tokia situacija akcentuoja, kad reikia patikimų privatumo išsaugojimo mechanizmų visame DI mokymo procese.

Teoriniuose darbuose dar labiau kvestionuojama dvinarė anonimiškumo samprata. Wachter ir Mittelstadt (2018) siūlo kontekstinę anoniminių duomenų sistemą, kurioje atsižvelgiama į priešininko galimybes, duomenų rinkinio savybes ir numatomą duomenų naudojimą. Tai dera su didėjančiu siekiu užtikrinti "pritaikytąją duomenų apsaugą" pagal BDAR 2 str. 25, kuriame akcentuojamos integruotos apsaugos priemonės, o ne *post hoc* anoniminių duomenų vertimo bandymai. Mantelero ir Esposito (2021) palaiko šį požiūrį, pristatydami įrodymais pagrįstą poveikio žmogaus teisėms vertinimo (angl. Human Rights Impact Assessments, HRIA) metodiką, pritaikytą dirbtinio intelekto kūrimui. Jų metodikoje pabrėžiamas dinaminis vertinimo modelis, kuris vystosi kartu su BPDI sistemų gyvavimo ciklu, pabrėžiant adaptyvių apsaugos priemonių ir skaidrumo mechanizmų, galinčių spręsti kylančią riziką, susijusią su pakartotiniu duomenų tapatybės nustatymu, būtinybę.

Lyginamoji teisinė analizė atskleidžia ryškius požiūrių skirtumus. ES taikomas rizika grindžiamas atpažįstamumo testas, kuriuo užtikrinama, kad net ir pašalinus tiesioginius identifikatorius, pakartotinio atpažinimo rizika turi būti nereikšminga. Kita vertus, JAV sistemos dažnai vertina galimybę nustatyti tapatybę, remdamosi duomenų valdytojo

ketinimais ir galimybe nustatyti tapatybę duomenų tvarkymo metu. De Brouwer (2020) kritikuoja šį JAV teisėje vyraujantį individualistinį privatumo modelį, teigdamas, kad jame nepakankamai įvertinamas kolektyvinis privatumo rizikos pobūdis tarpusavyje susijusiose skaitmeninėse ekosistemose. Jo analizėje pabrėžiama, kaip vieno duomenų subjekto veiksmai, pavyzdžiui, sutikimas naudoti jo duomenis, gali netyčia pakenkti kitų asmenų privatumui, todėl sutikimu grindžiami modeliai yra nepakankami siekiant užtikrinti patikimą apsaugą BPDI kontekste. Dėl to atsiranda reguliavimo asimetrija, kai duomenų rinkiniui, kuris Kalifornijoje teisiškai klasifikuojamas kaip neasmeninis, gali būti taikomi BDAR įpareigojimai, jei jis naudojamas ES. Daugianacionaliniams BPDI paslaugų teikėjams dėl to sudėtinga užtikrinti atitiktį, ypač taikant vieną modelį, parengtą mišrių jurisdikcijų duomenų rinkiniams.

Apibendrinant galima teigti, kad anoniminiai ir pseudoniminiai duomenys suteikia dalines, dažnai pervertintas garantijas, apsaugančias nuo pakartotinio identifikavimo, ypač BPDI kontekste. Dėl didėjančios dirbtinio intelekto sistemų galios ir nepakankamo jurisdikcijų suderinimo tradicinės duomenų apsaugos priemonės tampa nepakankamos. Politika ir teisė turi būti plėtojama kartu su technologijomis, taikant prie rizikos prisitaikančias metodikas, integruojant etinį auditą ir nustatant įgyvendinamus techninius standartus. Kol tokios sistemos nebus visuotinai priimtos, BPDI sistemos ir toliau bus įtrauktos į teisinį netikrumą, o anonimiškumas bus labiau procedūrinė fikcija nei esminė apsauga.

2.3. ALGORITMŲ (NEMATOMOJO TURINIO AR KITAIP JUODOSIOS DĖŽĖS) PROBLEMA IR SKAIDRUMO IŠ VERSLŲ PUSĖS TRŪKUMAS

Algoritmų neskaidrumas, liaudiškai vadinamas "juodosios dėžės efektu", tapo pagrindine etine, teisine ir technologine problema bendrosios paskirties dirbtinio intelekto (BPDI) eroje. Šis terminas reiškia dirbtinio intelekto sistemoms, ypač toms, kurios sukurtos remiantis gilaus mokymosi architektūromis, būdingą sudėtingumą ir aiškumo trūkumą. Tokios sistemos gali savarankiškai mokytis iš didžiulių duomenų kiekių, tačiau jos nesugeba pateikti žmogui suprantamų savo rezultatų paaiškinimų. Dėl to asmenims sunku užginčyti automatizuotus sprendimus, o reguliavimo institucijoms - įvertinti atitiktį teisiniams standartams. Radanliev (2025) pabrėžia, kad BPDI "juodosios dėžės" pobūdis

kenkia demokratinei priežiūrai ir gali kelti egzistencinę grėsmę informacijos vientisumui ir visuomenės pasitikėjimui dirbtinio intelekto valdymu.

BPDI taikymas jautriose srityse, pavyzdžiui, sveikatos diagnostikoje, prognozuojamojoje policijos veikloje ir finansinėse paslaugose, didina poreikį skubiai kovoti su algoritmų neskaidrumu. Patil (2025) iliustruoja, kaip neskaidrus AI, naudojamas žmogiškųjų išteklių valdyme, gali atgaminti sisteminį šališkumą, lemiantį diskriminacinę įdarbinimo praktiką. Skaidrumo trūkumas ne tik daro poveikį teisingumui, bet ir kelia pavojų pažeisti antidiskriminacinius įstatymus. Corselli (2023), atlikdamas sisteminę apžvalgą, nustatė, kad dauguma aukšto lygio dirbtinio intelekto sistemų turi paaiškinamumo trūkumų, kurie trukdo žmogiškajai priežiūrai ir kelia teisinį susirūpinimą dėl atskaitomybės. Be to, Cheong (2024) teigia, kad toks neskaidrumas trukdo demokratiniam svarstymui, nes iš asmenų atimama teisė suprasti, kaip daromos dirbtiniu intelektu pagrįstos išvados.

ES ėmėsi ryžtingų veiksmų, kad sumažintų su algoritmų neskaidrumu susijusią riziką. Bendrojo duomenų apsaugos reglamento 2 straipsnyje asmenims suteikiama teisė nepriimti sprendimų, grindžiamų tik automatizuotu duomenų tvarkymu. Šią nuostatą papildo 71 konstatuojamoji dalis, kurioje reikalaujama pateikti reikšmingą informaciją apie logiką, susijusią su tokiais sprendimais. Be to, siūlomame AI įstatyme BPDI sistemos priskiriamos "didelės rizikos" sistemoms, o paslaugų teikėjams nustatomi išsamūs dokumentavimo, testavimo ir skaidrumo įpareigojimai. Thanasas, Kampiotis ir Karkantzou (2025) pažymi, kad šios priemonės atspindi ES atsargumo principą, kuriuo siekiama apsaugoti pagrindines teises skaitmeninėje srityje. Tačiau Chung (2024) kritikuoja praktinį "teisės į paaiškinimą" įgyvendinimą, atkreipdamas dėmesį į atotrūkį tarp teisinių ketinimų ir technologinių galimybių. Daugelis BPDI kūrėjų remiasi komercinės paslapties išimtimis, todėl naudotojams sunku veiksmingai pasinaudoti savo teisėmis pagal BDAR.

Jungtinėse Amerikos Valstijose taikomas reguliavimo metodas yra visiškai priešingas. Nors Kalifornijos vartotojų privatumo įstatyme CCPA ir jo pakeitimuose, priimtuose CPRA, numatytos tam tikros naudotojo teisės, pavyzdžiui, teisė žinoti, ištrinti duomenis ir atsisakyti dalytis duomenimis, jose nenumatyta formalizuota "teisė į paaiškinimą", panaši į BDAR. Nonju ir Ihua-Maduenyi (2024) pabrėžia, kad dėl tokio reguliavimo fragmentiškumo dirbtinio intelekto bendrovėms suteikiama didelė veiksmų laisvė nustatant savo sistemų skaidrumo lygį. Praktikoje tai lemia minimalią atskaitomybę ir menką paskatą teikti paaiškinimus. Šią problemą dar labiau apsunkina tai, kad nėra

federalinės dirbtinio intelekto sistemos, todėl valdymas priklauso nuo konkrečiam sektoriui taikomų taisyklių, pavyzdžiui, nustatytų FTC ar FDA.

Be to, Cole (2024) nagrinėja šios transatlantinės atskirties poveikį pasauliniam valdymui. Jų analizė rodo, kad reglamentavimo skirtumai sudaro sąlygas "jurisdikcijos pasirinkimui", kai įmonės naudojasi švelnesnėmis jurisdikcijomis, kad paleistų dirbtinio intelekto sistemas, kurios kitur gali neatitikti griežtesnių skaidrumo ribų. Šis pasaulinis priežiūros atotrūkis tampa ypač problemiškas BPDI priemonėms, parengtoms pagal tarptautinius duomenis ir diegiamoms tarpvalstybiniu mastu. Siekdami užkirsti tam kelią, mokslininkai ir politikos formuotojai pasisako už tarptautinį reguliavimo derinimą. Paaiškinamasis dirbtinis intelektas (XAI) - sparčiai besivystanti mašininio mokymosi sritis - siūlo technines priemones, nes pirmenybė teikiama skaidrumui ir aiškinamumui neaukojant našumo. Kaip pažymi Cheong (2024), šios inovacijos yra labai svarbios siekiant suderinti AI plėtrą su žmogaus teisių įsipareigojimais.

Be to, kiti nauji moksliniai tyrimai atskleidžia kolektyvinę neskaidrių dirbtinio intelekto sistemų keliamą riziką. Ehimuan (2024) įvardija algoritmų neskaidrumą kaip struktūrinę kliūtį privatumo teisės aktų vykdymui, ypač besivystančiose jurisdikcijose. Savo moksliniame straipsnyje ji taip pat pabrėžia, kad neskaidrios sistemos griauna informuotą sutikimą, kuris yra šiuolaikinių duomenų apsaugos režimų kertinis akmuo. Tuo tarpu Leslie (2024) teigia, kad BPDI sustiprina jau egzistuojančią galios asimetriją tarp technologijų bendrovių ir naudotojų, todėl, prisidengus "dirbtinio intelekto inovacijomis", galima nekontroliuojamai kaupti duomenis. Šios įžvalgos sustiprina poreikį skaidrumą įtvirtinti ne tik reguliavimo lygmeniu, bet ir dirbtinio intelekto sistemų projektavimo etape.

Apibendrinant galima pasakyti, kad algoritmų neskaidrumas tebėra didžiulis iššūkis siekiant etiško ir teisėto dirbtinio intelekto. Nors ES sukūrė išsamią teisinę struktūrą juodosios dėžės problemai spręsti, vykdymo užtikrinimas atsilieka nuo technologinės pažangos. Ir atvirkščiai, JAV modelis suteikia lankstumo naudotojų apsaugos ir skaidrumo sąskaita. Norint užpildyti šias spragas, reikia dvigubos strategijos: plėtoti tarptautinį bendradarbiavimą reguliavimo srityje ir skatinti XAI metodų integravimą į dirbtinio intelekto kūrimo procesus. Tik užtikrinus skaidrumą projektuojant ir teisės aktais nustatytą galimybę atlikti auditą, BPDI sistemos gali pasitarnauti visuomenei nepakenkdamos jos demokratiniams ir teisiniams pagrindams.

3. POPULIARIAUSIŲ BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO SISTEMŲ ATITIKTIES DUOMENŲ APSAUGOS REIKALAVIMAMS VERTINIMAS

Per pastaruosius penkerius metus sparčiai plintant BPDI sistemoms, atsirado didelių skaitmeninių inovacijų, personalizavimo ir produktyvumo galimybių. Tačiau duomenų apdorojimo mastas ir neskaidrumas, susijęs su tokiais modeliais kaip „ChatGPT“, „Claude“, „Gemini“, „Copilot“, „Perplexity AI“ ir „LexisNexis“ analizės platformos, paskatino duomenų apsaugos institucijų, pareigūnų, teisininkų ir teisės mokslininkų vis didesnę kontrolę. Kadangi šios sistemos yra apmokytos iš didžiulių ir įvairialypių duomenų rinkinių, dažnai paimtų iš atviro interneto arba gautų iš asmeninių naudotojų sąveikų, jos kvestionuoja pagrindinius duomenų apsaugos principus pagal ES BDAR ir CCPA bei CPRA. Reguliavimo požiūriu BDAR yra išsamiausia sistema, pagal kurią galima įvertinti BPDI atitiktį. BDAR 5 ir 6 straipsniuose pabrėžiami sąžiningumo, teisėtumo, skaidrumo ir tikslo ribojimo principai. Tačiau BPDI sistemos dažnai nesuteikia galutiniams naudotojams pakankamai informacijos apie tai, kokie asmens duomenys yra renkami, kaip jie tvarkomi ir kokiais aiškiais tikslais. Pasak Cartwright, Dunbar ir Radcliffe (2024), net populiariausių platformų, tokių kaip ChatGPT ir Gemini, privatumo politikoje pateikiami neaiškūs arba pernelyg techniški aprašymai, o tai riboja naudotojų supratimą apie tai, kaip jų užklausos gali būti saugomos, analizuojamos ar pakartotinai panaudojamos.

Europos duomenų apsaugos valdyba (EDPB, 2024 m.) pabrėžia iššūkį, kurį kelia kalbos modeliai, veikiantys pagal bendrosios paskirties teiginius. Šiuose modeliuose dažnai supriešinami ir duomenų tvarkytojų, ir duomenų valdytojų vaidmenys, todėl kyla teisinių dviprasmybių dėl atskaitomybės. Nesant aiškaus asmens duomenų tvarkymo teisinio pagrindo, ypač tokių jautrių kategorijų, kaip politinės nuomonės ar biometriniai duomenų identifikatoriai, įterpti į tekstines užuominas, BPDI teisėtumas pagal BDAR išlieka abejotinas. Nors tokie paslaugų teikėjai kaip „Claude“ pabrėžia saugumą pagal dizainą ir mažesnę haliucinacijų riziką, empiriniai vertinimai rodo, kad nė viena iš aukščiausio lygio platformų nuosekliai neįgyvendina BDAR atitinkančios duomenų minimizavimo praktikos (Barbera, 2025).

Šis iššūkis dar didesnis jurisdikcijose, kuriose galioja sektoriniai arba fragmentiški privatumo įstatymai, pavyzdžiui, Jungtinėse Amerikos Valstijose. Nors CPRA sustiprino vartotojų teises ir įsteigė Kalifornijos privatumo apsaugos agentūrą (CPPA), išlieka didelė vykdymo užtikrinimo spraga. Šių trūkumų pavyzdys - LexisNexis. Kaip dokumentuoja

Needle ir Rubel (2023), LexisNexis partnerystė su teisėsaugos institucijomis, įskaitant Imigracijos ir Muitinės tarnybą (angl.: Immigration and Customs Enforcement, ICE), atskleidžia sisteminius sutikimo gavimo ir tinkamo proceso laikymosi trūkumus, dėl kurių kartu su privatumo pažeidimais kyla konstitucinių klausimų. LexisNexis dirbtiniu intelektu paremtose priemonėse integruojama realaus laiko analizė ir didžiuliai komercinių duomenų rinkiniai, tačiau jose pateikiama mažai informacijos apie duomenų kilmę ar atsisakymo procedūras, todėl pažeidžiami pranešimo ir naudotojo kontrolės principai, kurie yra svarbiausi ir BDAR, ir CPRA.

Kiti pagrindiniai rinkos dalyviai, pavyzdžiui, „Microsoft Copilot“ ir „Google Gemini“, sulaukė kritikos dėl riboto skaidrumo, susijusio su automatinėmis išvadomis, antrinių duomenų naudojimu ir dalijimosi duomenimis su trečiųjų šalių plėtiniais ar įskiepiais pobūdžiu. Kaip Informacijos komisaro biuras (ICO, 2024 m.) pažymi „Microsoft 365 Copilot“ DPIA peržiūroje, daugelis dirbtinio intelekto funkcijų veikia kaip „juodosios dėžutės“ patobulinimai, uždėti ant įmonės programinės įrangos, apeinant standartinius audito ir sutikimo protokolus. Panašiai Hoitingh (2025) pastebi, kad „Copilot“ integravimas į kasdienes produktyvumo priemones normalizuoja aplinkos duomenų rinkimą, dar labiau nutrindamas ribas tarp naudotojo ketinimų ir organizacijos profiliavimo.

„Perplexity“ DI, nors ir palyginti naujas, taip pat kelia nemažai rūpesčių. Valchanovas (2025) nurodo, kad nors „Perplexity“ naudoja šaltinio priskyrimą ir bando pateikti skaidrius paieškos rezultatus, jame nėra aiškios duomenų kontrolės mechanizmų. Vartotojai nėra aiškiai informuojami, ar jų paieškos užuominos naudojamos mokymui, taip pat nėra intuityvių atsisakymo galimybių. Dėl to „Perplexity“ prieštarauja BDAR 13 ir 14 straipsnių reikalavimams dėl skaidraus informavimo ir tikslo nurodymo. Jos privatumo politikoje nenurodomi duomenų saugojimo terminai, anoniminių duomenų vertimo metodai ar trečiųjų šalių duomenų gavėjų kategorijos. Šie iššūkiai pabrėžia platesnę tendenciją: didelės talpos BPDI sistemų ir nepakankamos atitikties architektūros susiliejimą. Nors techninės inovacijos dažnai lenkia teisinį reguliavimą, BPDI kūrėjai privalo laikytis privatumo užtikrinimo pagal projektą požiūrio. Tačiau, pasak Barberos (2025) ir Ehimuano (2024), daugumoje BPDI platformų trūksta pro-aktyvių poveikio duomenų apsaugai vertinimų ir tik nedaugelyje jų įdiegti patikimi mechanizmai, palengvinantys prieigos prie informacijos, informacijos ištaisymo ar duomenų ištrynimo teises. Vietoj to pramonės praktikoje dominuoja ne informuoto sutikimo, o dviprasmiško „teisėto intereso“ ar naudotojų licencijų susitarimai.

Be to, ankstesniuose skyriuose aptartas dirbtinio intelekto rezultatų „juodosios dėžės“ pobūdis didina naudotojų profiliavimo ir automatinio vertinimo riziką. Tokios BPDI sistemos kaip Claude ir Copilot vis dažniau padeda rengti dokumentus, atsakyti į jautrius klausimus ir teikti rekomendacijas. Tačiau šios rekomendacijos gali būti susijusios su „Inference“ analize, kuri profiliuoja naudotojus be jų žinios. McFarland, A. (2024) praneša, kad Claude atsakymų modeliai labai skiriasi priklausomai nuo naudotojo užklausų, o tai gali reikšti, kad jos algoritme įdiegtas elgsenos modelių atpažinimas. Toks profiliavimas - ypač kai jis taikomas komerciniame ar viešojo sektoriaus kontekste - gali būti laikomas automatizuotu sprendimų priėmimu pagal BDAR 22 straipsnį.

Galiausiai, tarptautinis duomenų apsaugos sistemų susiskaidymas apsunkina vykdymo užtikrinimą. Nors ES BDAR ir būsimasis DI aktas siūlo normatyvines taisykles, dauguma BPDI pardavėjų yra įsikūrę JAV, kur vykdymo užtikrinimas priklauso nuo bylinėjimosi, atskirų valstijų įstatymų ir savanoriško jų laikymosi. Šis neatitikimas sudaro sąlygas "reguliaciniam arbitražui", kai įmonės diegia modelius visame pasaulyje, tačiau tik minimaliai laikosi vietos teisinių reikalavimų. Vis dažniau pasigirsta raginimų derinti transatlantinius standartus, nes reguliavimo institucijos pripažįsta, kad būtina skubiai suvienodinti skaidrumo, duomenų lokalizavimo, algoritmų turinio atskaitomybės ir žmogiškosios priežiūros standartus (Ehimuan ir kt., 2024).

Apibendrinant galima daryti išvadą, kad pirmaujantys BPDI paslaugų teikėjai duomenų apsaugos sistemų laikosi iš dalies, nenuosekliai ir reaktyviai. Nors įmonės padarė laipsnišką pažangą atskleisdamos politiką ir integruodamos DPIA, vis dar esama esminių teisinių spragų duomenų tikslo aiškumo, automatinės išvados, skaidrumo ir naudotojų teisių gynimo mechanizmų srityse. Jei nebus nepriklausomo audito, aiškesnių DPIA šablonų ir suderintų pasaulinių standartų, etiškos ir teisėtos BPDI integracijos pažadas liks neįgyvendintas.

3.1. SAUGUMO UŽTIKRINIMO PRIEMONIŲ (NE)PAKANKAMAS TAIKYMAS (ŠIFRAVIMAS, PRIEIGOS KONTROLĖ IR DUOMENŲ SAVALAIKIS PANAIKINIMAS BEI KITI)

BPDI modelių saugumo aplinka tebėra viena svarbiausių, tačiau nepakankamai išvystytų privatumo reguliavimo sričių. Tiek ES, tiek Jungtinės Valstijos susiduria su precedento neturinčiais iššūkiais kuriant, įgyvendinant ir užtikrinant pakankamas saugumo apsaugos priemones dirbtinio intelekto ekosistemose. Šios sistemos, pavyzdžiui, „ChatGPT“, „Microsoft Copilot“, „Claude“ ir „Gemini“, nuolat gauna naudotojų duomenis, todėl kyla sudėtingų rūpesčių dėl saugaus saugojimo, teisėto tvarkymo ir galimo netyčinio pakartotinio asmenų tapatybės nustatymo. Naujausioje Millerio (2024) ataskaitoje pabrėžiama, kad šie modeliai paprastai diegiami komercinėje aplinkoje, visiškai neatsižvelgiant į kontekstui būdingą privatumo riziką, ypač kai naudotojai nežino, kaip jų užuominos ir sąveikos gali būti naudojamos pagrindiniams modeliams perkvalifikuoti ar patikslinti.

Asmens duomenų saugojimas tebėra viena iš pagrindinių saugumo problemų. Nors dauguma tiekėjų teigia, kad naudotojo duomenų nesaugo visam laikui, modelio atmintyje vis dar gali būti žurnalų, šešėlinių talpyklų ir išvadų įrašų. Pagal BDAR 17 straipsnį (teisė į ištrynimą) ir CPRA teisę ištrinti asmeninę informaciją, tokia praktika gali būti laikoma neteisėtu duomenų saugojimu, nebent ji būtų sušvelninta naudojant pažangius metodus, pavyzdžiui, trumpalaikę atmintį arba privačios sesijos užklausos formatą. Neseniai atskleista informacija apie ChatGPT modelio tikslinimą atskleidė, kad net nuasmeninti duomenys gali prisidėti prie mokymo duomenų, veiksmingai apeinant sutikimo reikalavimus (Miller, 2024). Be to, ištrynimo procesai debesijos pagrindu veikiančiose BPDI priemonėse stokoja reguliarių patikrinimų ir ne visada gali patvirtinti, ar naudotojo asmens duomenys yra visiškai pašalinti iš vidaus sistemų, todėl kyla teisinių dviprasmybių ir reguliavimo trinties.

Šifravimo mechanizmai tebėra pamatiniai, tačiau jų veiksmingumas labai priklauso nuo įgyvendinimo detalių. Nors dauguma BPDI platformų užtikrina TLS duomenų perdavimui, šifravimas atmintyje taikomas nenuosekliai, ypač trumpalaikiams duomenims, saugomiems gyvų modelių sesijų metu. Kaip parodyta Sikdar et al. (2024), įsilaužėliai gali pasinaudoti likutine prieiga prie atminties, kad atkurtų anksčiau įvestas užklausas ir taip netiesiogiai profiliuotų naudotoją. Šis pažeidžiamumas tampa ypač svarbus sektoriuose, susijusiuose su neskelbtinais sveikatos ar švietimo duomenimis, kur BDAR 9 straipsnyje ir

CPRA 1798.140 skirsnyje nurodyti konkretūs saugumo lūkesčiai. Nepaisant šių teisinių kriterijų, pagrindiniai pardavėjai, tokie kaip „Microsoft“, pripažino silpnąsias vietas taikant šifravimą ramybės būsenoje laikiniems metaduomenims, sukurtiems užpildant raginimus (Securiti.ai, 2024). Prieigos kontrolė „BPDI“ sistemose dar nėra tiek ištobulinta, kad būtų užtikrinta atitiktis teisės aktų reikalavimams. Tiek įmonėse, tiek vartotojui skirtose sistemose naudotojai dažnai sąveikauja su modeliais, įterptais į bendradarbiavimo platformas, tokias kaip „Slack“, „Zoom“ ar mokomosios informacinės lentelės. Nesant pritaikomosios prieigos politikos, gali kilti privilegijų didinimo atakų, kaip pabrėžiama keliuose Needle ir Rubel (2024 m.) atliktuose atvejų tyrimuose. Pavyzdžiui, jei naudotojo autentiškumo patvirtinimas tvarkomas taikomosios programos lygmeniu, bet nesustiprinamas BPDI sluoksnyje, gali būti daromos neleistinos išvados tarp sesijų. ES duomenų valdytojai pagal BDAR 32 straipsnį yra įpareigoti įdiegti tinkamas prieigos valdymo sistemas, o JAV sistemose, pavyzdžiui, CPRA, numatyti silpnesni vykdymo užtikrinimo standartai, pasikliaujant atsakomybe po įvykio, o ne iš ankstinio saugumo projektavimu.

Viena iš didžiausių BPDI saugumo architektūros spragų yra tai, kad nėra patikrinamų ištrynimo protokolų. BDAR saugojimo apribojimo principus ir CPRA nustatytus privalomus ištrynimo terminus sunku įgyvendinti, jei sistemose nėra ištrynimo įrodymo registravimo. Skirtingai nuo įprastų duomenų bazių, dideli kalbos modeliai neišlaiko statinių eilutės lygmens duomenų struktūrų, o tai reiškia, kad vieno duomenų įrašo ištrynimas gali nepanaikinti jo statistinės įtakos modelio svoriams. Neseniai paskelbtame Duffourc, Gerke ir Kollnig (2024) ir Sebastian (2023) darbe pasisakoma už „privatumą išsaugančių mokymo režimų“, kurie skirsto ir seka duomenų kilmę visuose mokymosi etapuose, kūrimą. Kol tokios architektūros nebus pritaikytos, saugumui išliks pavojus, kurį kelia ilgalaikė atmintis, įterpta į neauditуojamus modelio komponentus.

Paaiškinamumas ir interpretavimas dažnai aptariami etinio dirbtinio intelekto požiūriu, tačiau jie labai svarbūs saugumo užtikrinimui. Saugumo incidentai, kilę dėl nepaaiškinamų sprendimų, pavyzdžiui, neobjektyvių rezultatų, „haliucinuotų“ rekomendacijų arba netyčinio anksčiau įvestų užuominų nutekinimo, rodo, kad nepavyko užtikrinti skaidrumo ir patikimo dizaino. Wang (2024) tyrimuose pabrėžiama, kad į BPDI infrastruktūrą reikia įtraukti „atsekamumo modulius“, kad būtų galima saugiai atvaizduoti naudotojo įvestis ir modelio išvestis. Tokie moduliai galėtų padėti ir auditoriams, ir duomenų subjektams ginti savo teises pagal BDAR 15 straipsnį arba tikrinti CPRA privalomą atskleisti informaciją apie duomenų rinkimą ir naudojimą.

Be techninių apsaugos priemonių, taip pat reikia įvertinti institucines diegimo aplinkybes. Švietime ar sveikatos priežiūroje įdiegtos dirbtinio intelekto sistemos dažnai susiduria su kitokiais grėsmių modeliais nei elektroninės prekybos ar klientų aptarnavimo sistemos. Pavyzdžiui, sistemos, kuriomis naudojasi vaikai, gali rinkti duomenis, klasifikuojamus pagal BDAR 8 straipsnį (Nepilnamečių sutikimas), todėl reikia aukštesnio lygio autentiškumo nustatymo ir sutikimo registravimo. Ir atvirkščiai, JAV nepilnamečių duomenys tik iš dalies saugomi pagal COPPA, todėl tokiose aplinkose CPRA turi vykdymo užtikrinimo spragų. Dėl šios tarptautinės darnos stokos tarptautiniams BPDI pardavėjams sunku kurti universalius saugumo protokolus, todėl bendros apsaugos priemonės diegimo aplinkose yra silpnesnės (Duffourc et al., 2024).

Galiausiai, vertinant BPDI saugumo priemones reikia pereiti nuo statinių kontrolinių sąrašų vertinimų prie dinamiškų, rizika pagrįstų metodikų. Ir BDAR, ir CPRA dabar pripažįsta konteksto vaidmenį nustatant reikalingą saugumo lygį, ypač scenarijuose, susijusiuose su didelės apimties naudotojų sąveika, įvairių platformų integracija ir tolesniais duomenų srautais. Miller (2024) rekomenduoja įtraukti nuolatinį dirbtinio intelekto auditą, anomalijų aptikimo sistemas ir privatumą išsaugančius skaičiavimo metodus kaip besikeičiančią geriausią praktiką. Taip pat BDAR rizikos vertinimu pagrįsta atskaitomybės sistema, derinama su mašininiam mokymuisi pritaikytais DPIA (poveikio duomenų apsaugai vertinimais), galėtų tapti būsimų priežiūros mechanizmų reguliavimo pagrindu.

3.2. ETINIO DI PRINCIPŲ INTEGRAVIMAS Į BPDI SISTEMŲ KŪRIMĄ IR DIEGIMĄ

Besikeičiančioje skaitmeninėje aplinkoje etinis BPDI integravimas tapo daugiau nei reguliavimo reikalavimu - tai pagrindinis tvarių technologinių inovacijų ramstis. Kitaip nei ankstesniuose dirbtinio intelekto kūrimo etapuose, kai daugiausia dėmesio buvo skiriama našumui ir naudingumui, šiuolaikinės BPDI sistemos vis dažniau vertinamos pagal jų gebėjimą gerbti žmogaus teises, saugoti demokratines vertybes ir palaikyti sprendimų priėmimo procesų vientisumą. Dėl jų plataus pritaikymo teisinėje, akademinėje, verslo ir viešojoje srityse kyla svarbių etinių klausimų, kurie neapsiriboja atskiromis funkcijomis ar techniniu tikslumu. Mokslininkai dabar pabrėžia, kad etinių principų įtraukimas į BPDI sistemų kūrimą ir diegimą turi būti sistemingas, išmatuojamas ir atsparus komerciniam spaudimui (Floridi ir Cowls, 2019; Miller, 2024).

Dauguma komercinių BPDI teikėjų neskaidriai tvarko mokymo duomenų, algoritmo struktūros ir atnaujinimo procedūrų dokumentus, tačiau tik prioretizuojant skaidrumą galime užtikrinti etiškumą naudojant BPDI. Nors „OpenAI“ išleido ChatGPT modelių korteles ir politikos santraukas, kritikai teigia, kad šių priemonių nepakanka, kad būtų užtikrintas tikras aiškumas ar vieša atskaitomybė (Miller, 2024). Claude ir Gemini panašiai atskleidžia minimalią informaciją apie mokymo šaltinius, ypač apie turinio moderavimo mechanizmus ir modelių perkvalifikavimo dažnumą. Toks neskaidrumas trukdo veiksmingai įgyvendinti BDAR 5 straipsnio reikalavimus dėl skaidrumo ir kenkia CPRA 1798.110 straipsniui dėl prieigos prie vartotojų duomenų. Kaip pažymi Morley et al. (2023), skaidrumas turi būti suprantamas ne tik kaip pareiga atskleisti informaciją, bet ir kaip projektavimo principas, dėl kurio dirbtinio intelekto samprotavimai tampa suprantami ir reguliavimo institucijoms, ir naudotojams.

BPDI sistemos neišvengiamai perima ir sustiprina mokymo duomenų statistinius modelius, įskaitant istorinę neteisybę ir socialinę nelygybę, todėl natūraliai formuojasi tam tikro šališkumo apsireiškimai.. Neseniai atliktame Binns (2021) empiriniame tyrime pabrėžiama, kad didelių kalbos modelių generuojami rezultatai dažnai atspindi rasinius, lyčių ir kultūrinius šališkumus. Ypač „Microsoft Copilot“ ir „LexisNexis“ sulaukė kritikos dėl sisteminių šališkumų stiprinimo teisiniame ir įdarbinimo kontekste (Needle, Rubel, 2024). Teisėtvarkos, imigracijos ir prognozavimo policijos veiklos srityse šališki rezultatai gali lemti diskriminacinių sprendimų priėmimą, turintį realių pasekmių. Nors BDAR teisingumo principas įpareigoja aktyviai mažinti šališkumą, CPRA nėra algoritmais pagrįstų normatyvinių teisingumo gairių, todėl ES ir JAV jurisdikcijose etikos standartai yra fragmentiški.

Kita opi problema - naudotojų savarankiškumo mažėjimas. Dirbtinio intelekto generuojami atsakymai dažnai atrodo autoritetingi, net jei yra netikslūs, todėl naudotojai priima sprendimus remdamiesi klaidingais rezultatais. Pavyzdžiui, įrodyta, kad „Perplexity“ ir „Gemini“ teikia tikroviškai skambančius, bet faktiškai neteisingus teisinius ar medicininius patarimus (Wang, 2023). Tokie rezultatai kelia etinių abejonių dėl informuoto sutikimo ir naudotojų kontrolės, susijusios su algoritmų įtaka. Floridi ir Cowls (2019) teigia, kad etiškas dirbtinis intelektas turi išsaugoti žmogaus veiksnumą, užtikrindamas, kad naudotojai galėtų panaikinti, kvestionuoti arba atsisakyti automatinių pasiūlymų. Šiuo atžvilgiu AI akte numatyta rizika pagrįsta klasifikavimo sistema suteikia struktūrizuotą sistemą, pagal kurią, atsižvelgiant į taikymo kontekstą, priskiriami etiniai įsipareigojimai - standartas, kuris šiuo metu neatsispindi JAV reguliavimo srityje.

Atsakomybė yra bene sunkiausiai pasiekiamas etinis principas diegiant BPDI. Įmonės retai kada skaidriai informuoja, kaip į modelių atnaujinimus įtraukiami naudotojų atsiliepimai ir ar reguliariai atlieka etinio poveikio vertinimus. Bendrovės „Claude“, „ChatGPT“ ir „Copilot“ remiasi sustiprinto mokymosi iš žmogaus atsiliepimų (angl.: reinforcement learning from human feedback, RLHF) formomis, tačiau neatskleidžia savo klaidų taisymo modulių ar valdymo struktūros, prižiūrinčios modelio perkvalifikavimą (Securiti.ai, 2024). Kaip teigia Mantelero ir Esposito (2021), atskaitomybės mechanizmai turi apimti išorės auditą, aiškias atsakomybės ribas ir vykdytinas teisių gynimo priemones. Pagal BDAR 24 straipsnį duomenų valdytojai turi įrodyti, kad aktyviai laikosi reikalavimų, pateikdami dokumentus ir atlikdami rizikos vertinimą - reikalavimai, kurie daugelyje komercinių AI pasiūlymų vis dar nepakankamai išvystyti. Priešingai, BDAR daug dėmesio skiriama vykdymo užtikrinimui po pažeidimo, todėl sumažėja ex ante atskaitomybės mechanizmų, kurie yra svarbiausi etiškam BPDI diegimui, taikymo sritis.

Jautrumas kontekstui yra dažnai nepastebimas, tačiau etikos požiūriu labai svarbus aspektas. BPDI sistemos dažnai apibendrina savo elgesį įvairiose taikymo srityse, neatsižvelgdamos į naudotojų lūkesčių, teisinių pasekmių ar kultūrinių normų skirtumus. Toks universalus požiūris gali būti problemiškas, ypač kai jis taikomas tokiuose sektoriuose kaip švietimas, sveikatos priežiūra ar teisinės paslaugos. Pavyzdžiui, „Perplexity“ ir „LexisNexis“ apibendrina įvairių sričių duomenis be tinkamų etinių apribojimų konkrečiai sričiai. Mokslinėje literatūroje vis dažniau pasisakoma už kontekstą atitinkančias projektavimo sistemas, įskaitant diferencijuotas privatumo ribas, sutikimu pagrįstą personalizavimą ir dinaminį rizikos modeliavimą (Mantelero, Esposito, 2021; Duffourc et al., 2024). ES reglamentavimo aplinka remia šias pastangas per DPIA įgaliojimus ir tikslo apribojimo reikalavimus, o JAV reglamentavimas atsilieka kodifikuojant tokią geriausią praktiką.

Apibendrinant galima teigti, kad etinė BPDI sistemų integracija yra daugialypė užduotis, reikalaujanti daug daugiau nei paviršutiniškos atitikties ar *ad hoc* savireguliacijos. Kad etikos normos tikrai atitiktų demokratijos principus, pagrindines teises ir visuomenės lūkesčius, jos turi būti institucionalizuotos per visą DI gyvavimo ciklą - nuo duomenų rinkinių atrankos ir algoritmų architektūros iki diegimo aplinkos ir grįžtamojo ryšio ciklų. Kaip parodyta šioje analizėje, pirmaujančios platformos, tokios kaip „ChatGPT“, „Claude“, „Gemini“, „Copilot“, „Perplexity“ ir „LexisNexis“, atskleidžia ir etinį potencialą, ir sistemines silpnąsias vietas. Jų diegimas kritiniuose sektoriuose pabrėžia, kad skubiai reikia įgyvendinti skaidrumo, sąžiningumo, atskaitomybės ir kontekstinio jautrumo standartus.

Akademiniai tyrimai nuolat rodo, kad modeliai, parengti be etinių apsaugos priemonių, yra linkę atkartoti struktūrinius šališkumus, klaidinti naudotojus ir duoti neskaidrius rezultatus, kurie trukdo teisinei gynybai (Binns, 2021; Mantelero, Esposito, 2021). Siekiant pašalinti šiuos trūkumus, koordinuotomis kūrėjų, reguliavimo institucijų, tyrėjų ir pilietinės visuomenės pastangomis pirmenybė turi būti teikiama etikos principams, griežtiems poveikio vertinimams ir nepriklausomiems priežiūros mechanizmams. Tik tada BPDI sistemos gali tapti patikimais, teisingais ir patikimais šiuolaikinės informacinės visuomenės komponentais.

4. TEISMŲ PRAKTIKA IR DUOMENŲ APSAUGOS INSTITUCIJŲ REKOMENDACIJOS BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO DUOMENŲ APSAUGOS SRITYJE

Kadangi BPDI sistemos toliau vystosi ir integruojasi tiek į privačią, tiek į viešąją sritį, nacionaliniai ir tarptautiniai teismai vis dažniau raginami spręsti teisinius ginčus dėl duomenų apsaugos pažeidimų. Šiais teismų sprendimais ne tik aiškinamos ir taikomos galiojančios teisinės sistemos, pavyzdžiui, BDAR ES ir CCPA/CPRA JAV, bet ir sukuriami precedentai, darantys įtaką būsimoms atitikties prievolėms ir reguliavimo raidai. Teismai veikia kaip itin svarbūs vertintojai nustatant BPDI praktikos teisėtumą, ypač susijusį su automatizuotu duomenų tvarkymu, profiliavimu ir neteisėtu asmens duomenų naudojimu. Jų sprendimai atspindi didėjantį susirūpinimą dėl inovacijų ir privatumo teisių, skaidrumo ir atskaitomybės pusiausvyros (Mantelero, Esposito, 2021). Šiame skirsnyje išsamiai nagrinėjami pasirinkti svarbiausi sprendimai, iliustruojantys, kaip teisminiai išaiškinimai formavo besikeičiantį supratimą apie teisėtą BPDI veikimą, ypač atsižvelgiant į asmens teises ir institucijų atsakomybę.

Nepaisant to, kad daugelis su BPDI susijusių klausimų yra nauji, įvairių jurisdikcijų teismai jau pradėjo apibrėžti atsakomybės šioje srityje kontūrus. ES kelios duomenų apsaugos institucijos ir teismai pabrėžė griežtą BDAR principų taikymą - ypač dėl teisėtų duomenų tvarkymo pagrindų ir teisės į paaiškinimus automatizuoto sprendimų priėmimo sistemose (Juliussen, 2025). Tuo tarpu Jungtinėse Amerikos Valstijose teismų praktika tebėra fragmentiška, atspindinti labiau sektorinį požiūrį į duomenų privatumą, kai teisminiai ginčai dažnai sutelkiami į apgaulingą veiklą, žalą vartotojams arba sutarčių pažeidimus (Newell et al., 2024). Šie skirtumai išryškina iššūkį pasiekti transatlantinio

nuoseklumo teisinėse reakcijose į BPDI ir kartu sustiprina lyginamosios teisinės analizės poreikį.

Vienas iš svarbių teismų dalyvavimo BPDI srityje bruožų - vis dažniau naudojami poveikio vertinimai ir techninės ekspertų nuomonės kaip teisinio pagrindimo dalis. Teismai nebesitenkina abstrakčiais atitikties patikinimais; vietoj to jie reikalauja akivaizdžių įrodymų apie privatumą pagal projektą, rizikos vertinimus ir žalos mažinimo strategijas (Mantelero, Esposito, 2021). Tai ypač akivaizdu Europoje, kur vykstant teisminiams ginčams dėl dirbtinio intelekto diegimo dažnai tikrinami poveikio duomenų apsaugai vertinimai. Tuo tarpu JAV teismai tik neseniai pradėjo svarstyti sistemines su BPDI susijusio duomenų tvarkymo pasekmes, dažnai remdamiesi deliktais grindžiamais argumentais arba vartotojų apsaugos teise, kad įvertintų, ar naudotojo duomenys buvo panaudoti netinkamai (FTC, 2024). Vystantis šiam teisminiam dialogui, teisinės sistemos palaipsniui tobulina standartus, pagal kuriuos vertinami BPDI galimybės ir sistemų operatoriai.

Galiausiai, šie teismų sprendimai nėra izoliuoti, juos dažnai lemia platesnė institucinė dinamika, įskaitant reguliavimo gaires ir besivystančias teisines doktrinas. Dinamiška teismų sprendimų ir teisės aktų aiškinimų sąveika prisideda prie vis sudėtingesnės teisinės ekosistemos, kurioje BPDI įmonės turi nuolat prisitaikyti prie teisinio neapibrėžtumo ir kartu išlaikyti inovacijų trajektoriją. Todėl tolesniuose poskyriuose aptarta teismų praktika yra ne tik ankstesnio vykdymo užtikrinimo registras, bet ir objektyvas, per kurį galima suprasti ir pritaikyti naujus teisinius lūkesčius.

4.1. BAUDŲ, UŽ DUOMENŲ APSAUGOS PAŽEIDIMUS BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO KONTEKSTE, PREVENCINIS POVEIKIS ES IR JAV JURISDIKCIJOSE

Duomenų apsaugos teisės aktų vykdymas skiriant administracines baudas yra labai svarbus komponentas užtikrinant teisės normų laikymąsi, ypač sparčiai besivystančiuose sektoriuose, pavyzdžiui, BPDI. Baudos tradiciškai tarnauja kaip atgrasomoji priemonė, parodanti organizacijoms apčiuopiamas reikalavimų nesilaikymo pasekmes. BPDI kontekste tokių sankcijų taikymas tampa dar svarbesnis dėl neskaidrios duomenų tvarkymo praktikos, tarpvalstybinio paslaugų pobūdžio ir sunkumų nustatant atskaitomybę automatizuoto sprendimų priėmimo grandinėse. ES BDAR duomenų apsaugos institucijoms suteikiami įgaliojimai skirti administracines baudas, siekiančias iki 4 %

įmonės metinės pasaulinės apyvartos. Šios baudos yra ne tik baudžiamosios, bet ir atlieka auklėjamąją funkciją, nes jomis nustatomi aiškūs precedentai ir standartai. Ryškus pavyzdys - Italijos duomenų apsaugos institucijos (Garante) 2025 m. „OpenAI“ skirta 15 mln. eurų bauda. Ši bauda ne tik pabrėžia BDAR reguliavimo griežtumą, bet ir nustato prevencinį etaloną, atgrasantį kitus BPDI teikėjus nuo panašios praktikos (Laher, 2025 m.).

Galimas tokių sankcijų poveikis neapsiriboja vien tik organizacija, kuriai taikomos sankcijos, bet sukuria precedentus, kurie daro įtaką konkurentų ir partnerių elgesiui. Ryškus šio prevencinio mechanizmo pavyzdys yra reikšmingas 2023 m. Airijos duomenų apsaugos komisijos sprendimas, kuriuo bendrovei „Meta Platforms Ireland Ltd.“ buvo skirta 1,2 mlrd. eurų bauda už neteisėtą duomenų perdavimą į Jungtines Amerikos Valstijas (DPC, 2023). Ši sankcija buvo grindžiama BDAR nuostatų dėl tarptautinio duomenų perdavimo pažeidimais, visų pirma pagal reglamento V skyrių. Šis sprendimas svarbus ne tik dėl baudos piniginės vertės, bet ir dėl platesnio atgrasomojo poveikio visai pramonei. Teisės mokslininkai mano, kad tai yra esminė priemonė siekiant priversti laikytis tarptautinių duomenų apsaugos garantijų, ypač tarp BPDI teikėjų, kurių modeliams dažnai reikalinga plati ir nuolatinė prieiga prie asmens duomenų. Priešingai, Jungtinėse Valstijose nėra vieno išsamaus federalinio duomenų apsaugos įstatymo. Teisės aktų vykdymas dažnai būna fragmentiškas, remiamasi konkretiems sektoriams skirtais įstatymais ir Federalinės prekybos komisijos (FTC) įgaliojimais. LexisNexis atveju bendrovė susidūrė su teisine kontrole dėl tariamo asmens duomenų pardavimo JAV imigracijos tarnyboms be tinkamo sutikimo ar skaidrumo. Nors šis ieškinys rodo didėjantį supratimą apie pavojų privatumui komercinių duomenų rinkose, vieningų teisinių standartų nebuvimas mažina atgrasomąjį poveikį, palyginti su ES (CBS News, 2024). Akademiniuose tyrimuose pabrėžiama, kad finansinės nuobaudos gali būti veiksmingos tik tada, kai jos suvokiamos kaip proporcingos ir neišvengiamos. Kuner ir kt. (2020) pažymi, kad baudų veiksmingumas pagal BDAR priklauso nuo jų nuoseklumo, nuspėjamumo ir integracijos su kitais vykdymo užtikrinimo mechanizmais, tokiais kaip auditas ir taisomieji nurodymai. Taip brėžiama aiški atskyrimo linija, kad baudos turėtų būti vertinamos ne atskirai, o kaip platesnės reguliavimo strategijos, apimančios suinteresuotųjų šalių įtraukimą ir atitikties užtikrinimo paskatas, dalis.

Tokiose jurisdikcijose kaip Vokietija ir Prancūzija nacionalinės duomenų apsaugos institucijos ėmėsi aktyvesnės pozicijos, atlikdamos prevencinius auditus ir viešai skelbdamos sprendimus dėl vykdymo užtikrinimo, susijusius su BPDI arba su dirbtiniu intelektu susijusia duomenų tvarkymo praktika. Vokietijos federalinis duomenų apsaugos

ir informacijos laisvės komisaras (BfDI) ypač pasisakė už baudų taikymą kartu su taisomaisiais įsakymais (EDPB, 2019). Šiuo daugiasluoksniu vykdymo užtikrinimo metodu siekiama užkirsti kelią pasikartojimui ir nukreipti organizacijas į atitikties kultūrą. Prancūzijos CNIL panašiai pabrėžė, kad baudomis turėtų būti ne tik baudžiama, bet ir šviečiamos suinteresuotosios šalys apie atsakingą AI praktiką. Teisminės institucijos vaidmuo aiškinant vykdymo užtikrinimo nuostatas taip pat yra labai svarbus. Naujausiuose Europos Sąjungos Teisingumo Teismo (ESTT) sprendimuose išaiškinta, kad automatizuotam profiliavimui didelės rizikos kontekste turi būti taikomos sustiprintos apsaugos priemonės, įskaitant individualizuotą žmogaus peržiūrą. Tokiais sprendimais užtikrinamas teisinis aiškumas ir kartu sustiprinamas administracinių baudų, kaip atitikties užtikrinimo priemonių, rimtumas. Panašiai ir nacionalinių teismų sprendimai rodo tendenciją griežčiau aiškinti skaidrumo ir sutikimo prievoles.

Be to, baudos turi būti pritaikytos taip, kad atspindėtų konkrečią BPDI keliamą riziką. Skirtingai nei tradiciniai duomenų valdytojai, BPDI modeliai mokomi iš didžiulių duomenų rinkinių, dažnai paimtų iš viešai prieinamų šaltinių be tinkamo įspėjimo ar sutikimo mechanizmų. Tai padidina neleistino duomenų tvarkymo riziką ir apsunkina atsakomybės priskyrimą. Kaip pabrėžia Waldas (2024), skiriant baudas BPDI kontekste reikia atsižvelgti į galimos žalos mastą ir sisteminį pobūdį, ypač kai asmens duomenys įtraukiami į modelio rezultatus arba naudojami algoritmų šališkumui sustiprinti. Praktiškai baudų prevencinė funkcija taip pat priklauso nuo teisminės kontrolės ir viešumo. Skaidrūs duomenų apsaugos institucijų sprendimai, kaip OpenAI ir Clearview AI bylose, padeda informuoti kitus dalyvius ir sustiprinti atskaitomybės standartus. Tačiau, kaip aptarė Lintvedt (2021), nenuoseklus vykdymo užtikrinimas skirtingose jurisdikcijose gali pakenkti šiam poveikiui. Pavyzdžiui, Lenkijos duomenų apsaugos institucija pradėjo tyrimą dėl ChatGPT, tačiau dar nepaskyrė jokių konkrečių sankcijų, todėl kyla klausimų dėl vykdymo užtikrinimo veiksmingumo ir tarpvalstybinio bendradarbiavimo (Lomas, 2023).

Taigi, nors baudos yra nepakeičiama BPDI reguliavimo priemonė, jų prevencinis veiksmingumas priklauso nuo daugelio veiksnių: teisinių įpareigojimų aiškumo, institucinių gebėjimų užtikrinti jų vykdymą, tarptautinės darnos ir visuomenės informuotumo. Atrodo, kad ES šiuo atžvilgiu siūlo labiau struktūrizuotą ir veiksmingą modelį, nors JAV pokyčiai rodo didėjančią konvergenciją, ypač per valstijų lygmens įstatymus ir bylinėjimosi strategijas.

4.2. SĖKMINGI / NESĖKMINGI ATVEJAI IR PAMOKOS, SUSIJUSIOS SU DUOMENŲ APSAUGOS PAŽEIDIMAIS BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO SISTEMOSE

Sėkmingų ir nesėkmingų BPDI duomenų apsaugos pažeidimų atvejų analizė suteikia svarbių įžvalgų apie praktinį reguliavimo standartų vykdymą, ypač ES ir JAV jurisdikcijose. Šie atvejų tyrimai atskleidžia ne tik atitikties iššūkių apimtį ir mastą, bet ir iliustruoja, kaip niuansuotai duomenų apsaugos principus aiškina teismai ir priežiūros institucijos. Ypač iliustratyvi situacija jau anksčiau abstrakčiai aptartas atvejis, tai 15 mln. eurų bauda, kurią Garante (Italijos duomenų apsaugos institucija) 2025 m. pradžioje skyrė OpenAI. Atlikusi tyrimą Garante nustatė daugybę Bendrojo duomenų apsaugos reglamento BDAR pažeidimų, būtent susijusių su skaidrumo trūkumu, neteisėtu duomenų rinkimu mokymo ChatGPT tikslais ir mechanizmų, užtikrinančių rezultatų tikslumą, nebuvimą (Laher, 2025 m.). Šiame sprendime pabrėžiamas didėjantis ES reguliavimo institucijų atkaklumas užtikrinant duomenų teises BPDI ekosistemoje.

Lenkijos duomenų apsaugos institucija pradėjo oficialų tyrimą dėl „OpenAI“, remdamasi vietos informatikos profesoriaus skundu, kuriame teigiama, kad „ChatGPT“ generavo klaidingus asmens duomenis ir neturėjo veikiančio koregavimo mechanizmo (Lomas, 2023). Šis skundas, kartu su ankstesniais Garante veiksmais, išryškina ES besikeičiančią tendenciją: nacionalinės reguliavimo institucijos vis dažniau reaguoja į individualius skundus ir yra susirūpinusios dėl BPDI sistemų tikslumo ir ištaisymo mechanizmų. Tokie tyrimai grindžiami BDAR 16 ir 17 straipsniais, kuriais užtikrinama teisė į ištaisymą ir ištrynimą, tačiau BPDI modeliai dažnai sunkiai vykdo šias pareigas dėl decentralizuoto ir tikimybinio modelio rezultatų pobūdžio. Dėl šių priežasčių vykdymo užtikrinimo bylose išryškėja svarbi doktrininė įtampa tarp naujoviško duomenų naudojimo ir duomenų subjekto teisių.

Lygiagrečiai vykstantys pokyčiai Jungtinėse Amerikos Valstijose atspindi labiau suskaidytą reguliavimo aplinką. Nors nėra federalinio įstatymo, panašaus į BDAR, tačiau valstijų lygmeniu imtasi veiksmų, kuriais pradėtas formuoti BPDI valdymas. Kalifornijos vartotojų privatumo agentūra (CCPA), vadovaudamasi CCPA reguliavimu ir išplėstiniu jo variantu CPRA, paskelbė automatizuotų sprendimų priėmimo technologijų, įskaitant BPDI, gaires. Tačiau priešingai nei ES nuosekli vykdymo užtikrinimo sistema, JAV teisinė aplinka tebėra reaktyvi ir dažnai sprendžia žalos klausimą tik po incidento. Nepaisant to, pagal Biometrinės informacijos privatumo įstatymą (toliau – „**BIPA**“), ypač Ilinojaus

valstijoje, iškelta keletas grupinių ieškinių, kuriuose ginčijama, kaip BPDI bendrovės tvarko biometrinius ir asmens identifikatorius be informuoto asmens sutikimo. Šios bylos rodo didėjantį teismų norą kvestionuoti neskaidrią duomenų tvarkymo praktiką ir nustatyti ribas naujoms dirbtinio intelekto technologijoms.

Kitas svarbus aspektas, susijęs su vykdymo užtikrinimu, yra duomenų apsaugos pažeidimai ir saugumo incidentai, kurie pabrėžia su BPDI susijusią operacinę riziką. Visų pirma, 2023 ir 2024 m. užfiksuoti keli incidentai, susiję su „ChatGPT“, „Copilot“ ir kitomis dirbtinio intelekto sistemomis, kai kurie iš jų buvo susiję su laikinu naudotojų pokalbių ir raginimų istorijų nutekėjimu. Šie incidentai atskleidė prieigos kontrolės, registravimo mechanizmų ir BPDI teikėjų naudojamų sistemos programavimo modulių integracijų pažeidžiamumą (Wald.ai, 2024 m.). Šie nesklandumai paskatino reguliavimo institucijų priežiūrą, o kai kurios ES duomenų apsaugos institucijos paskelbė preliminarias išvadas, kuriose teigiama, kad nepakankamas rizikos vertinimas ir silpnos saugumo apsaugos priemonės yra BDAR 32 straipsnio pažeidimas. JAV tokie incidentai atnaujino raginimus priimti federalinius dirbtinio intelekto teisės aktus ir įkvėpė konkrečiam sektoriui skirtus pasiūlymus, kuriuose daugiausia dėmesio skiriama dirbtinio intelekto paslaugų kibernetinio saugumo standartams.

Platesnė mokslinė literatūra patvirtina nuomonę, kad veiksmingas vykdymo užtikrinimas ir bylų analizė yra labai svarbūs BPDI ekosistemos teisėtumui. Remiantis išsamiu tyrimu, kurį paskelbė Golda et al. (2024), reguliavimo spragos ir nenuoseklios techninės apsaugos priemonės tebėra vieni svarbiausių iššūkių siekiant privatumo atitikties BPDI aplinkoje. Tyrime pabrėžiama, kad reikia suderinti rizikos klasifikavimo kriterijus įvairiose jurisdikcijose ir sukurti vykdymo užtikrinimo koalicijas, galinčias kovoti su tarptautiniais BPDI teikėjais. Teisės mokslininkai taip pat pabrėžia, kad reikia atlikti poveikio vertinimus, pritaikytus unikaliai rizikai, kurią kelia tikimybėmis pagrįsti kalbos modeliai, ir sukurti mechanizmus, kurie leistų audituoti ir tikrinti jų atitiktį duomenų apsaugos principams.

Teisminė priežiūra taip pat atlieka svarbų vaidmenį nustatant teisėto dirbtinio intelekto naudojimo ribas. Pavyzdžiui, Izraelio Aukščiausiasis Teismas paskelbė svarbią nuomonę, kurioje įspėjo teisininkus apie riziką, kylančią dėl galimų „haliucinuotų“ bylų citatų ir teisinių argumentų, kai procesiniuose dokumentuose remiamasi BPDI sukurtu turiniu (Ravia, Hammer, 2025). Nors šis sprendimas tiesiogiai neįgyvendina BDAR ar JAV privatumo įstatymų, jis atspindi platesnį teisminį BPDI apribojimų pripažinimą ir kontekstinės bei žmogaus vykdomos priežiūros būtinybę, ypač tokiose jautriose srityse kaip

teisė ir medicina. Ši byla paskatino tolesnes diskusijas Europos Žmogaus Teisių Teisme ir JAV teisės akademiniuose sluoksniuose dėl mašinų generuojamų teisinių argumentų etinio priimtinumo.

Iš šių atvejų galima pasimokyti. Pirma, vykdymo užtikrinimas atlieka prevencinę funkciją, nes skatina BPDI kūrėjus priimti privatumo užtikrinimo pagal projektą strategijas, atlikti rizikos vertinimus ir sukurti skundų nagrinėjimo mechanizmus. Antra, vykdymo užtikrinimas skatina visuomenės pasitikėjimą ir atskaitomybę atsirandančiomis dirbtinio intelekto technologijomis, o tai labai svarbu atsižvelgiant į galimą riziką visuomenei. Trečia, koordinuotais vykdymo užtikrinimo veiksmais visose ES valstybėse narėse galima suderinti pagrindinių BDAR nuostatų aiškinimą ir taip sumažinti teisinį netikrumą. Galiausiai, priešingas požiūris JAV atskleidžia, kad bendrosios teisės jurisdikcijose BPDI reguliavimo srityje gali dominuoti bylinėjimasis, o ne administracinis vykdymo užtikrinimas. Šie skirtumai taip pat atveria erdvę mišriems sprendimams, pavyzdžiui, viešojo ir privačiojo sektorių partnerystei arba trečiųjų šalių audito mechanizmams, kuriais siekiama didinti skaidrumą ir atitiktį.

Apibendrinant galima teigti, kad teismų praktika ir reguliavimo tyrimai, susiję su BPDI, atspindi vis ryžtingesnę ES reguliavimo poziciją, priešingai nei JAV, kur požiūris yra labiau reaktyvus ir fragmentiškas. Iš šių bylų išmoktos pamokos rodo, kad BPDI paslaugų teikėjai turi priimti aktyvias atitikties strategijas, taikyti privatumo užtikrinimo pagal dizainą principus ir įgyvendinti patikimus žalos atlyginimo mechanizmus. Keičiantis teisinei aplinkai, abiem jurisdikcijoms gali būti naudinga abipusė geriausios praktikos sklaida, derinant ES reglamentavimo įžvalgumą su JAV skiriamu dėmesiu inovacijoms ir konkrečiam sektoriui būdingam bylinėjimuisi.

4.3. DUOMENŲ APSAUGOS INSTITUCIJŲ GAIRĖS IR REKOMENDACIJOS DĖL BENDROSIOS PASKIRTIES DIRBTINIO INTELEKTO REGULIAVIMO, KAIP JOS FORMUOJA VARTOTOJŲ SUPRATIMĄ APIE GALIMUS PAVOJUS

Europos duomenų apsaugos valdyba (toliau – „**EDPB**“) yra viena iš pagrindinių institucijų, formuojančių ES požiūrį į asmens duomenų apsaugą BPDI kontekste. Savo gairėse EDPB pateikia teisiškai nuoseklų BDAR aiškinimą ir nurodo, kaip jo principus galima suderinti su atsirandančiais dirbtinio intelekto modeliais. Savo 2025 m. pseudoniminių duomenų gairėse EDPB dar kartą patvirtino, kad pseudoniminiai duomenys, nors pagal juos tiesiogiai

neidentifikuojami asmenys, BDAR taikoma ir toliau, jei pakartotinis identifikavimas yra pagrįstai įmanomas (EDPB, 2025). Šis išaiškinimas daro didelę įtaką tam, kaip BPDI kūrėjai ir duomenų valdytojai tvarko naudotojų įvestį, ypač kai dideli kalbos modeliai išsaugo informacijos fragmentus, kuriuos vėliau galima pakartotinai identifikuoti arba panaudoti.

Be pseudonimų suteikimo, EDPB pabrėžia duomenų kiekio mažinimo ir tikslo apribojimo principą. BPDI sistemos pagal savo konstrukciją dažnai renka ir apdoroja didelius tekstinių ar įvairialypio pobūdžio paieškos duomenų kiekius. Pasak EDPB, toks duomenų rinkimas visada turi būti proporcingas, būtinas ir aiškiai pagrįstas pagal BDAR 5 straipsnį. EDPB taip pat pabrėžia skaidrumo svarbą ir ragina geriau informuoti galutinius naudotojus apie tai, kaip naudojami jų duomenys, ypač išvestinių rezultatų atvejais. Mokslininkai pritarė EDPB pozicijai, teigdami, kad be griežtų reguliavimo aiškinimų BPDI sistemos gali paversti pagrindinius BDAR principus neveiksmingais. Pavyzdžiui, Kuner ir kt. (2020) pabrėžia, kad pseudonimų suteikimas turi būti laikomas apsaugos priemone, bet ne licencija neribotam duomenų tvarkymui. EDPB aktyviai skelbiami techniniai dokumentai taip pat padeda išaiškinti praktines BPDI naudojančių duomenų valdytojų pareigas. Be to, institucinis EDPB ir nacionalinių priežiūros institucijų bendradarbiavimas leido užtikrinti nuoseklios politikos vykdymą visose valstybėse narėse. Šis decentralizuotas, bet suderintas modelis leidžia EDPB vadovauti technologijų diegimui atsižvelgiant į nacionalinius teisinius ypatumus.

Jungtinėse Amerikos Valstijose Kalifornijos privatumo apsaugos agentūra (CPPA) vadovauja pastangoms reglamentuoti duomenų tvarkymą pagal CCPA ir CPRA. Nors šie įstatymai skiriasi nuo BDAR savo pagrindine logika - jie labiau grindžiami teisėmis ir orientuoti į rinką - CPPA paskelbė gaires, kuriose išreiškiamas panašus susirūpinimas dėl skaidrumo, vartotojų teisių ir tikslo apribojimo dirbtinio intelekto programose. CPPA viešos konsultacijos ir suinteresuotųjų šalių seminarai 2023 ir 2024 m. atskleidė didėjantį susirūpinimą dėl to, kaip BPDI priemonės, tokios kaip ChatGPT ir Gemini, tvarko neskelbtiną informaciją. Visų pirma CPPA pabrėžė, kad automatiniam sprendimų priėmimui reikia „pranešimo rinkimo metu“ ir išsamių atsisakymo mechanizmų. CPPA taip pat siekia užtikrinti tinkamą taisyklės „neparduoti ir nesidalyti“ taikymą - nuostatos, kuria dažnai remiamasi bylose, susijusiose su elgsenos profiliavimu arba BPDI duomenų saugojimo praktika. Akademiniuose komentaruose teigiama, kad CPPA pozicija, palyginti su EDPB, tebėra šiek tiek neišplėtota. Nors CPVA stiprina asmens teises, vykdymo užtikrinimo mechanizmai ir praktinės gairės atsilieka. Ši reguliavimo spraga atveria erdvę

nenuosekliam teisės taikymui įvairiose platformose. Nepaisant to, CPPA laikomas potencialiu pavyzdžiu kitoms JAV valstijoms, rodančiu laipsnišką, bet ryžtingą perėjimą prie tvirtesnio AI valdymo šalies viduje. Nepaisant šių iššūkių, CPPA dokumentai atspindi didėjantį supratimą apie BPDI būdingą riziką. Pavyzdžiui, CPPA seminaruose buvo pabrėžiama modelio audito galimybės ir atitikties CPRA duomenų saugojimo nuostatoms būtinybė. Agentūros bendravimas su pilietinės visuomenės grupėmis, privatumo gynėjais ir BPDI kūrėjais taip pat rodo, kad agentūra yra pasiryžusi prisitaikyti ir reaguoti į poreikius.

Be EDPB ir CPPA, formuojant duomenų apsaugos dialogą apie BPDI technines galimybes, labai svarbus vaidmuo teko ir kitoms įstaigoms. Informacijos politikos lyderystės centras (CIPL) ir Europos duomenų apsaugos organizacijų konfederacija (toliau – „CEDPO“) išleido baltąsias knygas, kuriose pabrėžiama rizika grindžiamo požiūrio ir duomenų valdymo svarba. CEDPO ataskaitoje apie bendrosios paskirties dirbtinio intelekto poveikį duomenų apsaugai (2023 m.) pabrėžiami praktiniai klausimai, pavyzdžiui, sunkumai įgyvendinant naudotojų teises transformatoriais grindžiamose architektūrose. Joje rekomenduojamos standartizuotos sąsajos duomenų subjektų prašymams ir griežtesnės kūrėjų prievolės atlikti poveikio duomenų apsaugai vertinimus (DPIA).

Be to, teisminės valdžios atstovai pradėjo viešai kalbėti šiais klausimais. Jungtinės Karalystės Rolls magistras (Master of the Rolls) paskelbė kalbas, kuriose perspėjo dėl vis dažniau naudojamo haliucinacinio turinio teisiniuose procesiniuose dokumentuose, kuriuos rengia dirbtinio intelekto sistemos. Tai išryškina platesnį susirūpinimą dėl automatizuotų teisinės pagalbos priemonių atskaitomybės ir patikrinimo. Tokie pokyčiai pabrėžia didėjančią teismų etikos svarbą valdant dirbtinio intelekto sistemas. Harmonic Security (2024 m.) analizėje taip pat pastebima nerimą kelianti netyčinių duomenų nutekėjimo tendencija BPDI platformose, iliustruojanti institucinius iššūkius, susijusius su duomenų valdymo palaikymu dideliu mastu. Straipsnyje nurodomi įvairūs pažeidžiamumai - nuo darbo užmokesčio duomenų atskleidimo iki konfidencialių intelektinės nuosavybės duomenų pateikimo, todėl reguliavimo institucijos raginamos reikalauti iš kūrėjų aiškesnės dokumentacijos ir operacinių apsaugos priemonių. Tęsiant nuodugnų institucinių ir ekspertinių atsakų į bendrosios paskirties dirbtinio intelekto reguliavimą tyrimą, šiame skyriuje plačiau aptariamas kitų įtakingų duomenų apsaugos institucijų ir akademinių institucijų vaidmuo. Toliau analizuojama, kaip šios organizacijos formuluoja reguliavimo prioritetus, leidžia atitikties priemones ir daro įtaką visuomenės informuotumui bei politikos formavimui. Taip pat akcentuojamas skirtingų Europos Sąjungos ir Jungtinių

Amerikos Valstijų interpretacijų, susijusių su dirbtinio intelekto etika, naudotojo sutikimu, rizikos vertinimu ir duomenų minimizavimu BPDI įrankių aplinkoje, suderinimas.

Besikeičiant bendrosios paskirties dirbtinio intelekto (BPDI) aplinkai, duomenų apsaugos institucijos (DAI) visoje Europoje ir Jungtinėse Amerikos Valstijose vis aktyviau reiškia susirūpinimą ir siūlo sistemas. Prancūzijos CNIL (Commission nationale de l'informatique et des libertés) 2023 m. paskelbė strateginį planą, kuriame išdėstytas laipsniškas požiūris į BPDI reguliavimą, pradedant nuo gilesnio duomenų srautų ir modelių elgsenos supratimo, vėliau atliekant techninius mokomųjų duomenų rinkinių auditus ir galiausiai užtikrinant skaidrumo prievolių vykdymą. Šiam sisteminiam požiūriui pritarė ir Vokietijos federalinis duomenų apsaugos ir informacijos laisvės komisaras (BfDI), kuris pasisako už privalomus rizikos vertinimus ir privatumo užtikrinimo pagal projektą principus prieš pradedant diegti BPDI.

Be to, Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) paragino parengti specialų BPDI reguliavimo priemonių rinkinį, į kurį būtų įtraukti dinamiški sutikimo mechanizmai ir konkrečiam dirbtiniam intelektui skirti poveikio vertinimo šablonai. Manoma, kad šios priemonės yra labai svarbios aplinkoje, kurioje tradicinių duomenų apsaugos priemonių, tokių kaip naudotojo sutikimas ir duomenų kiekio mažinimas, nepakanka išvestinių duomenų generavimui ir kryžminiam kontekstiniam nustatymui. Pasisakydamas už duomenų fiduciarinę atsakomybę, EDAPP pritaria tokiems mokslininkams kaip Mantelero, Esposito (2021), kurie teigia, kad etinės rizikos vertinimai turėtų būti institucionalizuoti įstatymuose, siekiant užtikrinti tvarų dirbtinio intelekto valdymą.

Tuo pat metu JAV institucijos, pavyzdžiui, Baltųjų rūmų Mokslo ir technologijų politikos biuras (toliau – „**OSTP**“), paskelbė neprivalomas, bet įtakingas sistemas, kuriose pirmenybė teikiama vartotojų apsaugai, algoritmų atskaitomybei ir teisingai prieigai. OSTP parengtame 2022 m. dirbtinio intelekto teisių įstatymo projekte pabrėžiama saugių ir veiksmingų sistemų, algoritmų diskriminacijos apsaugos ir prasmingų žmogiškųjų alternatyvų automatizuotiems sprendimams svarba. Nors šis dokumentas nėra teisiškai vykdytinas, jis formuoja diskursą ir stiprina poreikį, kad dirbtinio intelekto sistemos gerbtų asmens autonomiją ir duomenų agentūrą. Akademinis diskursas papildo šias institucines pastangas, atskleisdamas nuolatines įgyvendinimo spragas. Taeihagh 2025). apžvalgoje pabrėžiama, kad, nepaisant didėjančio sąmoningumo, veiklos skaidrumas išlieka nepasiekiamas dėl intelektinės nuosavybės pretenzijų ir komercinės paslapties. Be to, empiriniuose tyrimuose, kuriuos Stanfordo HAI centre atliko King, Meinhardt (2024 m.),

pabrėžiama neproporcingai didelė našta, tenkanti asmenims suprasti, įvertinti ir užginčyti automatizuotus sprendimus. Todėl teisės mokslininkai vis dažniau ragina kurti kolektyvinio privatumo modelius ir įstatymiškai pripažinti grupinę žalą, kylančią dėl netinkamo BPDI naudojimo.

Be nacionalinių ir žemyno institucijų, vis didesnį pagreitį įgauna transatlantinis bendradarbiavimas. ES ir JAV prekybos ir technologijų taryba (TTC) ir ES ir JAV mokslinių tyrimų aljansas sudaro darbo grupes, kuriose daugiausia dėmesio skiriama BPDI valdymo principų derinimui. Šiomis diskusijomis siekiama sumažinti reguliavimo susiskaidymą derinant standartus, susijusius su duomenų perkėlimo, auditu ir etiška AI plėtra. Nors rezultatai kol kas yra preliminarūs, jie rodo, kad vis labiau artėjama prie bendros atsakomybės mažinant su dirbtiniu intelektu susijusią privatumo riziką. Todėl pilietinės visuomenės organizacijų, tokių kaip NOYB (None of Your Business) (2024a), siūlomos įžvalgos rodo didėjantį teisinio aktyvumo vaidmenį formuojant BPDI atskaitomybę. NOYB (2024b) teisiniai ieškiniai prieš pagrindinius dirbtinio intelekto paslaugų teikėjus dėl BDAR neatitinkančios duomenų tvarkymo praktikos atskleidžia atotrūkį tarp deklaruojamų politinių ketinimų ir faktinio įmonių elgesio. Šios intervencijos dažnai tampa katalizatoriumi oficialiems DAI tyrimams ir stumia reguliavimo ribas į priekį. Todėl jos rodo dinamišką institucinės priežiūros, akademinių tyrimų ir pilietinės gynybos sąveiką platesnėje BPDI ekosistemoje.

5. IŠVADOS

Magistro darbe dėl didelės aptartų sričių įvairovės ir siekiant nuosekliai išdėstyti rezultatus, išvados yra formuluojamos sąrašo principu.

- Vis plečiama BPDI aplinka kelia sudėtingų iššūkių esamiems duomenų apsaugos režimams abiejų jurisdikcijų atžvilgiu. Nors tokiose reguliavimo sistemose, kaip BDAR ir CPPA, nustatyti pagrindiniai privatumo ir atskaitomybės principai, jos nebuvo sukurtos atsižvelgiant į dinamišką, savaime besimokantį BPDI sistemų pobūdį. Todėl jų taikymas šioms technologijoms tebėra ribotas, ypač atsižvelgiant į duomenų tvarkymo, susijusio su BPDI kūrimu ir diegimu, bei jų pritaikymo mastą ir neskaidrumą. Dėl asmens duomenų integravimo į modelio algoritmus dažnai tampa praktiškai neįmanoma užtikrinti pagrindinių duomenų subjekto teisių, tokių kaip sužinojimas savo duomenų, ištaisymas ir ištrynimas, laikymosi.
- Europos Sąjungos požiūris, įtvirtintas BDAR ir sustiprintas ES DI aktu, atspindi griežtesnį ir sistemiškesnį duomenų valdymo modelį, palyginti su JAV taikomu fragmentuotu valstijų lygmens reguliavimu. ES reguliavime pirmenybė teikiama asmens teisėms ir akcentuojamas skaidrumas, tikslo ribojimas ir atsakomybė. Tuo tarpu CCPA ir toliau remiasi reguliavimu grindžiamu aktyviais vartotojų veiksmais, tokiu požiūriu duomenų apsaugos naštą užkraunant asmenims, o ne nustatant įpareigojimus DI rinkos lyderiams. Tai lemia silpnesnę JAV vykdymo užtikrinimo aplinką ir nenuoseklų privatumo apsaugos priemonių taikymą įvairiose DI platformose.
- Atsakomybę BPDI ekosistemose kardinaliai apsunkina duomenų apdorojimo grandinėse dalyvaujančių subjektų įvairovė. Dėl neryškaus skirtumo tarp duomenų valdytojų ir duomenų tvarkytojų sunku veiksmingai atskirti kuriam iš jų tenka didesnė teisinė atsakomybė. Esamos teisinės sąvokos, apibrėžimai tiek ES, tiek ir JAV lygiu nėra lengvai pritaikomi prie decentralizuoto ir adaptyvaus BPDI kuriamų rezultatų ir jo galimybių, todėl atsiranda šių sistemų valdymo ir vykdymo užtikrinimo spragų. Tai lemia komplikuotą DI reguliavimo ir reglamentavimo aplinką, kurioje atsakomybė už duomenų apsaugą yra dažnai išsklaidyta tarp skirtingų subjektų ir todėl dažnu atveju neprisiimama.
- Informacijos šifravimas ir kodavimas, ilgą laiką DI rinkos lyderių laikyti veiksmingomis duomenų apsaugos strategijomis, vis tobulėjant LLM modeliams atskleidė, kad BPDI kontekste tinkamai paveikus sistemas, galima išgauti netgi ir

jautrius duomenis apie vartotojus. Šiuolaikinių modelių skaičiavimo galimybės didina duomenų pakartotinio identifikavimo galimybę, net ir iš duomenų rinkinių, kurie anksčiau buvo laikomi saugiais. Didelės dimensijos mokymo duomenų naudojimas ir įsiminimo galimybė LLM modeliuose dar labiau griauna prielaidą, kad užkoduotų duomenų nebegalima susieti su asmenimis. Dėl to pasikliaujant šiais mechanizmais be nuolatinio pakartotinio vertinimo, kuris yra privalomas vis sparčiau keičiantis BPDI galimybėms, kyla didelė rizika kiekvieno vartotojo duomenų privatumui.

- Dėl BPDI sistemų skaidrumo trūkumo, kuris dažnai vadinamas „juodosios dėžės“ problema, iš esmės apsunkinamas duomenų apsaugos principų įgyvendinimas. Šioms DI sistemoms trūksta aiškumo, galimybių jų veikimo principus paaiškinti, o tai trukdo naudotojams suprasti, kvestionuoti ar prieštarauti automatizuotiems sprendimams vartotojų atžvilgiu. Nors BDAR reglamente nustatyti skaidrumo įpareigojimai ir teisė nebūti išimtinai automatizuotai tvarkomų duomenų subjektu, dėl techninių BPDI apribojimų ir stambių DI rinkos lyderių pasipriešinimo vis dar sunku užtikrinti BDAR įtvirtintų principų vykdymą. Kadangi JAV reguliavime nėra panašios teisės į paaiškinimą dėl tvarkomų duomenų, ši problema tampa dar aktualesnė, todėl vartotojai turi dar labiau ribotas galimybes kontroliuoti savo duomenis ar jų pagrindu gautus rezultatus.
- Galiausiai, tarptautinis duomenų apsaugos įstatymų išsiskyrimas, skirtingas požiūris į DI reguliavimo svarbą palengvina BPDI valdytojų atitiktį. BPDI sistemas kuriančios organizacijos dažnai savo atitikties užtikrinimo pastangas pritaiko prie mažiausiai ribojančios jurisdikcijos, o tai daro neigiamą įtaką duomenų apsaugos standartų universalumui. Nesant suderintų reguliavimo metodų, atsiranda teisinis netikrumas, trukdoma užtikrinti griežtesnės jurisdikcijos normų vykdymą ir bendrai susilpnina naudotojų apsaugą. Šiems skirtumams pašalinti reikia ne tik teisėkūros reformų, ne tik bausti BPDI rinkos lyderius, bet ir tarpvalstybinio bendradarbiavimo bei požiūrio į DI derinimą, kad būtų užtikrinta, jog duomenų apsaugos teisės būtų nuosekliai ginamos tarptautiniu lygmeniu.

6. LITERATŪROS SĄRAŠAS

Teisės norminiai aktai:

1. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016, p. 1-88.
2. Europos Parlamento ir Tarybos 2024 m. birželio 13 d. reglamentas (ES) 2024/1689 kuriuo nustatomos suderintos dirbtinio intelekto taisyklės ir iš dalies keičiami reglamentai (EB) Nr. 300/2008, (ES) Nr. 167/2013, (ES) Nr. 168/2013, (ES) 2018/858, (ES) 2018/1139 ir (ES) 2019/2144 bei direktyvos 2014/90/ES, (ES) 2016/797 ir (ES) 2020/1828 (Dirbtinio intelekto aktas) OJ L, 2024/1689, 2024.
3. California Consumer Privacy Act of 2018, California USA (2018). 1798.100 - 1798.199.100
4. California Privacy Protection Agency (2023). Lawdivision 6. California privacy protection agencychapter 1. California consumer privacy act regulationsfinal regulations text (p. 1–66).
5. California Privacy Protection Agency (2024). Lawdivision 6. California privacy protection agencychapter 1. California consumer privacy act regulationsfinal regulations text (p. 1–67).
6. The White House (2022). Blueprint for an AI Bill of Rights: Making automated systems work for the American people. [interaktyvus].
7. European Commission (2021). Regulation of the European Parliament and of the Council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. 2021/0106(COD)

Specialioji literatūra:

8. Article 29 Data Protection Working Party (2013). Opinion 03/2013 on purpose limitation (p. 1–70). [interaktyvus]. http://ec.europa.eu/justice/data-protection/index_en.htm
9. Applying Data Protection Principles to Generative AI: Practical Approaches for Organizations and Regulators. (2024) [interaktyvus].

https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_applying_data_protection_principles_BPDI_dec24.pdf

10. Barberá, I. (2025). AI Privacy Risks & Mitigations Large Language Models (LLMs) [interaktyvus]. https://www.edpb.europa.eu/system/files/2025-04/ai-privacy-risks-and-mitigations-in-llms.pdf
11. Binns, R. (2020). On the apparent conflict between individual and group fairness. Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency, 514–524 [interaktyvus]. https://doi.org/10.1145/3351095.3372864
12. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. International Journal of Law and Information Technology, 27(2), 1–29 [interaktyvus]. https://doi.org/10.1093/ijlit/eay017
13. Carlini, N., Hayes, J., Nasr, M., Jagielski, M., Sehwag, V., Tramèr, F., Balle, B., Ippolito, D., & Wallace, E. (2023). Extracting training data from diffusion models. Proceedings of the 32nd USENIX Conference on Security Symposium, 1–19 [interaktyvus]. https://doi.org/10.48550/arXiv.2301.13188
14. Cartwright, O., Dunbar, H., & Radcliffe, T. (2024). Evaluating Privacy Compliance in Commercial Large Language Models - ChatGPT, Claude, and Gemini [interaktyvus]. https://doi.org/10.21203/rs.3.rs-4792047/v1
15. Cheong, B. C. (2024). Transparency and accountability in AI systems: safeguarding wellbeing in the age of algorithmic decision-making. Frontiers in Human Dynamics, 6, 1–1 [interaktyvus]. https://doi.org/10.3389/fhumd.2024.1421273
16. Chung, N. C., Chung, H., Lee, H., Brocki, L., Chung, H., & Dyer, G. (2024). False Sense of Security in Explainable Artificial Intelligence (XAI). 1–9 [interaktyvus]. https://doi.org/10.48550/arXiv.2405.03820
17. Corselli, E. (2023). The dark side of AI [Luleå University of Technology] [interaktyvus]. https://ltu.diva-portal.org/smash/record.jsf?pid=diva2%3A1811175&dswid=-6955
18. de Brouwer, S. (2020). Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation. Internet Policy Review, 9(4), 1–29 [interaktyvus]. https://doi.org/10.14763/2020.4.1537
19. Kuner, C. ir kt. (2020). The EU General Data Protection Regulation (GDPR): A Commentary (p. 292 – 302; 309 – 320; 555 – 581). Oxford University Press [interaktyvus]. https://doi.org/10.1093/oso/9780198826491.003.0031

20. Duffourc, M. N., Gerke, S., & Kollnig, K. (2024). Privacy of Personal Data in the Generative AI Data Lifecycle. NYU Journal of Intellectual Property & Entertainment Law, 13(2) [interaktyvus]. https://jipel.law.nyu.edu/privacy-of-personal-data-in-the-generative-ai-data-lifecycle/
21. Floridi, L., & Cowls, J. (2019). A Unified Framework of Five Principles for AI in Society. Harvard Data Science Review, 1, 1–15 [interaktyvus]. https://doi.org/10.1162/99608f92.8cd550d1
22. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., Luetge, C., Madelin, R., Pagallo, U., Rossi, F., Schafer, B., Valcke, P., & Vayena, E. (2018). AI4People—An Ethical Framework for a Good AI Society: Opportunities, Risks, Principles, and Recommendations. Minds and Machines, 28(4), 690–707 [interaktyvus]. https://doi.org/10.1007/s11023-018-9482-5
23. From Payrolls to Patents: The Spectrum of Data Leaked into BPDI. (2024) [interaktyvus]. https://www.harmonic.security/resources/from-payrolls-to-patents-the-spectrum-of-data-leaked-into-BPDI
24. Gasser, U., & Almeida, V. A. F. (2017). A Layered Model for AI Governance. IEEE Internet Computing, 21(6), 58–62 [interaktyvus]. https://doi.org/10.1109/MIC.2017.4180835
25. Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Wallach, H., Daumé, H., & Crawford, K. (2018). Datasheets for Datasets. 1–18 [interaktyvus]. https://arxiv.org/pdf/1803.09010
26. Gellert, R. (2020). Changes of regulatory models: From command and control to meta regulation. In The Risk-Based Approach to Data Protection (p. 1–27). Oxford University Press [interaktyvus]. https://doi.org/10.1093/oso/9780198837718.001.0001
27. Generative AI: The Data Protection Implications. (2023) [interaktyvus]. https://cedpo.eu/wp-content/uploads/generative-ai-the-data-protection-implications-16-10-2023.pdf
28. Golda, A., Mekonen, K., Pandey, A., Singh, A., Hassija, V., Chamola, V., & Sikdar, B. (2024). Privacy and Security Concerns in Generative AI: A Comprehensive Survey. IEEE Access, 12, 48126–48144 [interaktyvus]. https://doi.org/10.1109/ACCESS.2024.3381611
29. Hoofnagle, C. J., van der Sloot, B., & Zuiderveen Borgesius, F. (2018). The European Union General Data Protection Regulation: What It Is And What It

Means. SSRN Electronic Journal, 1–98 [interaktyvus]. https://doi.org/10.2139/ssrn.3254511

30. Hovy, D., & Spruit, S. L. (2016). The Social Impact of Natural Language Processing. In K. Erk & N. A. Smith (Eds.), Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 2: Short Papers) (p. 591–598). Association for Computational Linguistics [interaktyvus]. https://doi.org/10.18653/v1/P16-2096
31. Juliussen, B. A. (2025). MultiMedia Modeling. The Right to an Explanation Under the GDPR and the AI Act, 184–1197. https://link.springer.com/chapter/10.1007/978-981-96-2071-5_14
32. Kampiotis, G., Thanasas, G., & Karkantzou, A. (2025). Enhancing Transparency and Efficiency in Auditing and Regulatory Compliance with Disruptive Technologies. Theoretical Economics Letters, 15(1), 214–233 [interaktyvus]. https://doi.org/10.4236/tel.2025.151013
33. King, J., & Meinhardt, C. (2024). Rethinking Privacy in the AI Era Policy Provocations for a Data-Centric World [interaktyvus]. https://hai-production.s3.amazonaws.com/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf
34. Leslie, D., Ashurst, C., González, N., Griffiths, F., Jayadeva, S., Jorgensen, M., Katell, M., Krishna, S., Kwiatkowski, D., Martins, C., Mohammed, S., Mougan, C., Pandit, S., Richey, M., Sakshaug, J., Vallor, S., & Vilain, L. (2024). 'Frontier AI,' Power, and the Public Interest: Who Benefits, Who Decides? Harvard Data Science Review, 1–20 [interaktyvus]. https://doi.org/10.1162/99608f92.4a42495c
35. Lintvedt, M. N. (2022). Putting a price on data protection infringement. International Data Privacy Law, 12(1) [interaktyvus]. https://doi.org/10.1093/idpl/ipab024
36. Liu, Y, et al. (2024) Generative AI model privacy: a survey. [interaktyvus]. https://link.springer.com/article/10.1007/s10462-024-11024-6
37. Mantelero, A. (2018). AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. Computer Law and Security Review, 34(4), 754–772 [interaktyvus]. https://doi.org/10.1016/j.clsr.2018.05.017
38. Mantelero, A., Esposito, M. S. (2021). An evidence-based methodology for human rights impact assessment (HRIA) in the development of AI data-intensive systems.

Computer Law and Security Review, 41, 1–35 [interaktyvus]. https://doi.org/10.1016/j.clsr.2021.105561

39. Naghiyev, K. (2024). ChatGPT From a Data Protection Perspective. SSRN Electronic Journal, 10(1), 1–34 [interaktyvus]. https://doi.org/10.2139/ssrn.4579348
40. Needle, J., & Rubel, A. R. (2023). The ICE-Lexis Nexus: An argument against use of commercial databases in immigration enforcement [interaktyvus]. https://blogs.uoregon.edu/ssnoregon2023/abstracts/
41. European Data Protection Board (2025). Adopted-version for public consultation Guidelines 01/2025 on Pseudonymisation (p. 1–46). [interaktyvus]. https://www.edpb.europa.eu/system/files/2025-01/edpb_guidelines_202501_pseudonymisation_en.pdf
42. European Commission (2024). AI for public good: EU-U.S. research alliance in AI for the public good. [interaktyvus]. https://digital-strategy.ec.europa.eu/en/library/ai-public-good-eu-us-research-alliance-ai-public-good
43. European Data Protection Board (2020). Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1 (p. 1–33). [interaktyvus]. https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf
44. Newell, B. C., Purtova, N., Moon, Y. E., & Paterson, H. J. (2024). REGULATING THE DATA MARKET: THE MATERIAL SCOPE OF AMERICAN CONSUMER DATA PRIVACY LAW. University of Pennsylvania Journal of International Law, 45(4), 1134–1143 [interaktyvus]. https://doi.org/10.58112/jil.45-4.4
45. Nonju D.S K., & Ihua-Maduenyi, B. (2024). The Impact of Artificial Intelligence on Privacy Laws. International Journal of Research and Innovation in Social Science, 1–25 [interaktyvus]. https://doi.org/10.47772/IJRISS
46. Pahune, S., Akhtar, Z., Mandapati, V., & Siddique, K. (2025). The Importance of AI Data Governance in Large Language Models. Preprints, 1–39 [interaktyvus]. https://doi.org/10.20944/preprints202504.0219.v1
47. Patil, K., & Scholar II, R. (2025). Algorithmic Decision-Making in HR: Navigating Fairness, Transparency, and Governance in the Age of AI. INTERNATIONAL JOURNAL OF COMPUTER ENGINEERING & TECHNOLOGY, 16(1), 359–367 [interaktyvus]. https://doi.org/10.34218/IJCET_16_01_033

48. Radanliev, P. (2025). Frontier AI regulation: what form should it take? Frontiers in Political Science, 7, 1–17 [interaktyvus]. https://doi.org/10.3389/fpos.2025.1561776
49. Report of the work undertaken by the ChatGPT Taskforce. (2024) [interaktyvus]. https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf
50. Rocher, L., Hendrickx, J. M., & de Montjoye, Y. A. (2019). Estimating the success of re-identifications in incomplete datasets using generative models. Nature Communications, 10(1) [interaktyvus]. https://doi.org/10.1038/s41467-019-10933-3
51. Sarra, C. (2024). Artificial Intelligence in Decision-making: A Test of Consistency between the "EU AI Act" and the "General Data Protection Regulation." Athens Journal of Law, 11(7), 1–17 [interaktyvus]. https://doi.org/10.30958/ajl.11-1-3
52. Sebastian, G. (2023). Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information. International Journal of Security and Privacy in Pervasive Computing, 15(1), 1–14 [interaktyvus]. https://doi.org/10.4018/IJSPPC.325475
53. Taeihagh, A. (2025). Governance of Generative AI. Policy and Society, 44(1), 1–22 [interaktyvus]. https://doi.org/10.1093/polsoc/puaf001
54. TAM, J. (2024). Privacy law issues associated with developing and deploying generative AI tools. Privacy Law Section Journal, 1. [interaktyvus]. https://calawyers.org/privacy-law/privacy-law-issues-associated-with-developing-and-deploying-generative-ai-tools/
55. Tisné, M. (2020). The Data Delusion: Protecting Individual Data Isn't Enough When The Harm is Collective (M. Schaake, Trans.) [interaktyvus]. https://fsi9-prod.s3.us-west-1.amazonaws.com/s3fs-public/the_data_delusion_formatted-v3.pdf
56. Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data and Society, 4(2) [interaktyvus]. https://doi.org/10.1177/2053951717743530
57. Veale, M., & Borgesius, F. Z. (2021). Demystifying the Draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97–112 [interaktyvus]. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852

58. Wachter, S., & Mittelstadt, B. (2018). A RIGHT TO REASONABLE INFERENCES: RE-THINKING DATA PROTECTION LAW IN THE AGE OF BIG DATA AND AI. Columbia Business Law Review, 201(2), 1–130 [interaktyvus]. https://doi.org/10.31228/osf.io/mu2kf
59. Wang, T., Zhang, Y., Qi, S., Zhao, R., Xia, Z., & Weng, J. (2023). Security and Privacy on Generative Data in AIGC: A Survey [interaktyvus]. https://arxiv.org/html/2309.09435v2/#S3
60. Zaleskis, J. (2019). Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Registrų centras.
61. Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs [interaktyvus]. https://dn721805.ca.archive.org/0/items/zuboff-shoshana.-the-age-of-surveillance-capitalism.-2019/Zuboff%2C%20Shoshana.The%20Age%20of%20Surveillance%20Capitalism.2019.pdf

Teismų praktika:

Enciklopediniai, informaciniai ir statistiniai šaltiniai:

62. Yacomine, C. (n.d.). *Data Protection Impact Assessment (DPIA) – Microsoft CoPilot 365*. Retrieved April 1, 2025 [interaktyvus]. https://ico.org.uk/media2/ob4ncmpz/ic-359252-x5s0-copilot-dpia.pdf

Kiti šaltiniai:

63. AI and GDPR: the CNIL publishes new recommendations to suport responsible innovation. (2021, February 7). Commission Nationale de l'informatique et Des Libertés [interaktyvus]. https://cnil.fr/en/ai-and-gdpr-cnil-publishes-new-recommendations-suport-responsible-innovation

64. Alex McFarland. (2024, December 3). Claude Feature Enables Customized Writing Styles. Unite.Ai [interaktyvus]. https://www.unite.ai/claude-feature-enables-customized-writing-styles/
65. Artificial intelligence: the action plan of the CNIL. (2023, May 16). Commission Nationale de l'informatique et Des Libertés [interaktyvus]. https://www.cnil.fr/en/artificial-intelligence-action-plan-cnil
66. Baig, A. (2025, February 19). Understanding Microsoft Copilot Data Privacy Concerns. Securiti [interaktyvus]. https://securiti.ai/microsoft-copilot-privacy-concerns/
67. BfDI imposes Fines on Telecommunications Service Providers. (2019, December 18). European Data Protection Board [interaktyvus]. https://www.edpb.europa.eu/news/national-news/2019/bfdi-imposes-fines-telecommunications-service-providers_en
68. California Consumer Privacy Laws. (n.d.). Bloomberg Law. Retrieved April 1, 2025 [interaktyvus]. https://pro.bloomberglaw.com/insights/privacy/california-consumer-privacy-laws/#compliance
69. ChatGPT Data Leaks and Security Incidents (2023-2024): A Comprehensive Overview. (n.d.). Wald.Ai. Retrieved April 1, 2025 [interaktyvus]. https://wald.ai/blog/chatgpt-data-leaks-and-security-incidents-20232024-a-comprehensive-overview
70. Cole, M. (2024, July 9). Disconnected rules in a connected world: ideas for AI innovation and regulation. Reuters [interaktyvus]. https://www.reuters.com/legal/legalindustry/disconnected-rules-connected-world-ideas-ai-innovation-regulation-2024-07-09/
71. CPRA countdown: New compliance obligations and challenges around "sensitive personal information." (2021, February 11). Hogan Lovells [interaktyvus]. https://www.hoganlovells.com/en/publications/cpra-countdown-new-compliance-obligations-and-challenges-around-sensitive-personal-information
72. Data Protection Commission announces conclusion of inquiry into Meta Ireland. (2023, May 22). Data Protection Commission [interaktyvus]. https://www.dataprotection.ie/en/news-media/press-releases/Data-Protection-Commission-announces-conclusion-of-inquiry-into-Meta-Ireland
73. FTC Announces Crackdown on Deceptive AI Claims and Schemes. (2024, September 25). Federal Trade Commission [interaktyvus].

https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-announces-crackdown-deceptive-ai-claims-schemes

74. LexisNexis illegally collected and sold people's personal data, lawsuit alleges. (2022, August 16). CBS NEWS [interaktyvus]. https://www.cbsnews.com/news/lexisnexis-lawsuit-collected-sold-personal-data-immigration-advocates-allege/
75. Miller, K. (2024, March 18). Privacy in an AI Era: How Do We Protect Our Personal Information? Stanford University Human Centred Artificial Intelligence [interaktyvus]. https://hai.stanford.edu/news/privacy-ai-era-how-do-we-protect-our-personal-information
76. noyb urges 11 DPAs to immediately stop Meta's abuse of personal data for AI. (2024, June 6). Noyb [interaktyvus]. https://noyb.eu/en/noyb-urges-11-dpas-immediately-stop-metas-abuse-personal-data-ai
77. OpenAI faces €15 million fine as the Italian Garante strikes again. (2025, January 14). Lewis Silkin [interaktyvus]. https://www.lewissilkin.com/insights/2025/01/14/openai-faces-15-million-fine-as-the-italian-garante-strikes-again-102jtqc
78. Poland opens privacy probe of ChatGPT following GDPR complaint. (2023, September 21). Tech Crunch [interaktyvus]. https://techcrunch.com/2023/09/21/poland-chatgpt-gdpr-complaint-probe/
79. noyb WIN: Meta stops AI plans in the EU. (2024, June 14). Noyb [interaktyvus]. https://noyb.eu/en/preliminary-noyb-win-meta-stops-ai-plans-eu
80. Privacy Considerations for Generative AI. (n.d.). Office of the Chief Information Officer Privacy & Cybersecurity. Retrieved April 1, 2025 [interaktyvus]. https://www.cybersecurity.illinois.edu/policies-governance/privacy-considerations-for-generative-ai/
81. Ravia, H., & Hammer, D. (2025, March 31). Israeli Supreme Court Warns of AI Hallucinations in Pleadings. Pearl Cohen [interaktyvus]. https://www.pearlcohen.com/israeli-supreme-court-warns-of-ai-hallucinations-in-pleadings/
82. Tackling Microsoft 365 Copilot data security and governance concerns. (2025, January 20). Albert Hoitingh [interaktyvus]. https://alberthoitingh.com/2025/01/20/tackling-microsoft-365-copilot-data-security-and-governance-concerns/

83. Valchanov, I. (2025, February 12). Perplexity Review: Is It Worth It in 2025? [In-Depth]. Team GPT [interaktyvus]. https://team-gpt.com/blog/perplexity-review/

7. SANTRAUKA

Duomenų apsaugos ir dirbtinio intelekto suderinamumas: BDAR, ES DI aktas, CCPA ir kiti aktualūs teisės aktai

Adrianas Latvinskas

Magistro darbe kritiškai nagrinėjama bendrosios paskirties dirbtinio intelekto ir duomenų apsaugos suderinamumas, daugiausia dėmesio skiriama BDAR, ES DI įstatymui ir CCPA bei jo pakeitimui CPRA. Pagrindinis tikslas - įvertinti, kaip GenAI sistemos atitinka arba prieštarauja pagrindiniams privatumo principams, įskaitant tikslo apribojimą, duomenų minimizavimą, skaidrumą ir duomenų subjekto teises.

Analizė pradedama nuo konceptualaus ir teisinio asmens duomenų ir įvairių jų klasifikacijų paaiškinimo GenAI sistemų kontekste. Nagrinėjama, kaip GenAI įrankiai - tokie kaip ChatGPT, Claude, Gemini, Copilot ir LexisNexis - apdoroja tiek struktūrizuotus, tiek nestruktūrizuotus naudotojų duomenis, išskiriant jautrius asmeninius duomenis be aiškaus vartotojo sutikimo ar aiškiai atskleidžiant duomenų kilmę. Ypatingas dėmesys skiriamas tokiems pavojams kaip elgsenos profiliavimas, duomenų nutekėjimas ir netiesioginis pakartotinis tapatybės nustatymas. Empiriniais pavyzdžiais ir teismų praktika remiamasi analizuojant institucinę priežiūrą ir teisinį vykdymą. Darbe vertinami svarbūs reguliavimo veiksmai (pavyzdžiui, Garante's OpenAI tyrimas, Lenkijos DAI tyrimai) ir pagrindiniai teismų bei tarptautinių institucijų sprendimai. Atskaitomybės kartu su atsakomybe taikymas, juodosios dėžės problematikos atskleidimas ir išankstinių vertinimų, tokių kaip DPIA, inicijavimas, potencialiai vertinami kaip BPDI atitikties reguliavimo priemonės.

Be to, magistre vertinamos ir siūlomos apsaugos priemonės, kaip pseudonimų suteikimas, šifravimas ir etinės DI projektavimo sistemos, nustatant jų privalumus ir trūkumus. Taip pat lyginami ES ir JAV teisiniai požiūriai į skaidrumą, algoritmų atskaitomybę ir vykdymo užtikrinimo ribas, atskleidžiant esminius taikymo srities ir vykdymo užtikrinimo skirtumus. Tyrimas baigiamas struktūrizuotomis išvadomis, kuriose atskleidžiamas teisės aktų, etikos bei techninių sprendimų problematika ir siūloma stiprinti tarpvalstybinį bendradarbiavimą reguliavimo srityje.

8. SUMMARY

Data protection and AI compatibility: GDPR, EU IoT Act, CCPA and other relevant legislation

Adrianas Latvinskas

The Master's thesis critically examines the compatibility between general purpose AI and data protection, focusing on the GDPR, the EU's IoT law and the CCPA and its replacement CPRA. The main objective is to assess how GenAI systems comply or conflict with fundamental privacy principles, including purpose limitation, data minimisation, transparency and data subject rights.

The analysis starts with a conceptual and legal explanation of personal data and its various classifications in the context of the GenAI systems. It examines how GenAI tools - such as ChatGPT, Claude, Gemini, Copilot and LexisNexis - process both structured and unstructured user data, distinguishing sensitive personal data without explicit user consent or explicit disclosure of the origin of data. Particular attention is paid to risks such as behavioural profiling, data leakage and indirect re-identification. Empirical examples and case law are used to analyse institutional oversight and legal enforcement. The work assesses important regulatory actions (e.g. Garante's OpenAI study, the Polish DPA studies) and the main decisions of courts and international institutions. The use of accountability combined with responsibility, the exposure of black box issues and the initiation of pre-assessments such as DPIAs are potentially seen as regulatory tools for BPDI compliance.

In addition, the MSc also evaluates proposed safeguards such as pseudonymisation, encryption and ethical IoT design frameworks, identifying their advantages and disadvantages. It also compares the EU and US legal approaches to transparency, accountability of algorithms and enforcement thresholds, revealing key differences in scope and enforcement. The study concludes with structured conclusions, which highlight the challenges in terms of legislation, ethics and technical solutions, and propose to strengthen cross-border regulatory cooperation.