

Vilniaus universiteto

Filosofijos fakulteto

Magistro studijų programos „Taikomoji ir teorinė kriminologija“

Vaiva Žiogaitė

Taikomosios ir teorinės kriminologijos studijų programa

Magistro darbas

Algoritminių įrankių naudojimas, jų taikymo praktikos ir galimybės stiprinant
antikorupcinę aplinką

Darbo vadovė: Doc. Dr. Maryja Šupa

Vilnius

2024

Turinys

Santrauka	3
Summary.....	3
Įvadas	5
1. Algoritminių technologijų panaudojimas antikorupcinei aplinkai gerinti: norminis ir praktinis kontekstas	7
1.1 Algoritminių technologijų apibrėžimai	7
1.2. Algoritminės valdysenos iššūkiai	8
1.3. DI etikos principai bei jų problematika	10
1.4. Galima algoritminių įrankių naudojimo nauda korupcijos srityje	13
1.5. Galima algoritminių įrankių naudojimo žala korupcijos srityje	17
1.6. DI aktas – struktūra ir problematika	21
2. Algoritmai antikorupcinei aplinkai gerinti: dviejų pakopų metodas	23
2.1. Tyrimo metodika	23
2.2. Dokumentų analizė: ES šalių algoritmų technologijos antikorupcinės aplinkos gerinimo veikloje....	27
2.3. Kokybinis tyrimas: mokslininkų ir specialistų įžvalgos	32
2.4. Diskusija	41
Išvados	45
Rekomendacijos	46
Literatūra	48
1 priedas „Kodų ir subkodų medis“	54
2 priedas “ES šalių naudojamos algoritminės technologijos antikorupcinei aplinkai gerinti“	55

Santrauka

Sparčiai vystantis algoritminėms - dirbtinio intelekto (DI) technologijoms, atsiveria naujos galimybės skaidrumui, korupcijos rizikų valdymui bei darbui su jos reiškiniais. Tyrimų šia tema Lietuvoje – nėra, tuo tarpu užsienio literatūroje yra pasižymėjusių mokslininkų tyrinėjančių DI naudą, žalą bei panaudojimo galimybes antikorupcinei aplinkai gerinti. Šis tyrimas nagrinėja algoritminių įrankių taikymą antikorupcinės aplinkos stiprinimui – jų naudojimą, galimus iššūkius bei potencialą. Empirinio tyrimo metu analizuotos 27 ES šalys (nagrinėti 68 atvirųjų duomenų informacijos šaltiniai), atlikti 12 pusiau struktūruotų interviu (2 iš jų grupiniai, iš viso dalyvavo 16 asmenų) su DI srities mokslininkais bei specialistais, dirbančiais antikorupcinės aplinkos stiprinimo srityje. Pasitelkiant dokumentų analizę, rezultatai atskleidžia, kad algoritminiai sprendimai gausiai taikomi ES, įvairiose srityse: viešuosiuose pirkimuose, finansų sektoriuje bei biurokratijos naštai mažinti. Atliktas kokybinis tyrimas suteikė informacijos pagrindą apie sėkmingai pritaikomas technologijas, taip pat nurodė, kokie pavojai kyla taikant šias sistemas bei kokios sąlygos būtinos efektyviam šių technologijų integravimui. Lietuvoje algoritminių technologijų taikymas antikorupcinei aplinkai gerinti dar lėtas, tačiau egzistuoja tam tikri įrankiai, kurie jau dabar prisideda prie specialistų darbo spartinimo. Dažniausias naudojamas įrankis – generatyvusis DI, o aukštesnės rizikos sistemos Lietuvoje dar tik projektų stadijose. Interviu analizė taip pat išryškina esmines viešojo sektoriaus spragas: žinių, finansų, specialistų bei motyvacijos stoka. Surinkti duomenys tampa pagrindu suformuluoti įrodymais grįstas rekomendacijas tikslingai inovacijų plėtrai Lietuvos viešajame sektoriuje.

Summary

The rapid development of algorithmic – artificial intelligence (AI) technologies is opening new opportunities for transparency, managing corruption risks and dealing with corruption impacts. There are no studies on this topic in Lithuania; meanwhile, international literature features prominent scholars who explore the benefits, risks, and potential applications of AI in improving the anti-corruption landscape. This study examines the application of algorithmic tools to strengthen the anti-corruption environment - their use, possible challenges and potential. The empirical study analyzed 27 EU countries (68 open data information sources), conducted 12 semi-structured interviews (2 of them group interviews, with a total of 16 participants) with AI researchers and practitioners working on strengthening the anti-corruption environment. Through desk analysis, the results show that algorithmic solutions are widely used in the EU in a variety of areas such as public procurement, financial sector and to reduce the burden of bureaucracy. The qualitative research has provided a baseline of successful applications, as well as an indication of the risks involved and the conditions

necessary for the effective integration of these technologies. The study indicates that while the adoption of algorithmic technologies to improve the anti-corruption environment in Lithuania remains slow, some tools are already contributing to enhancing the work of professionals. The most commonly used tool is generative AI, while higher risk systems in Lithuania are still in the early stages of development. The analysis of the interviews also highlights key gaps in the public sector: lack of knowledge, finances, professionals and motivation. The data collected becomes the basis for formulating evidence-based recommendations for targeted innovation development in the Lithuanian public sector.

Ivadas

Korupcija kelia didelį iššūkį viso pasaulio visuomenėms, daro poveikį šalies valdymui, ekonominiam vystymuisi, socialiniam teisingumui ir teisinei valstybei (Transparency international, 2023). Norint veiksmingai užkirsti kelią korupcijai, reikia bendrų pastangų iš vyriausybių, pilietinės visuomenės ir tarptautinių organizacijų, kad būtų skatinamas skaidrumas, atskaitomybė ir sąžiningumas viešuosiuose procesuose. Dabartinėmis sąlygomis, kai nusikaltimai įgauna vis naujas formas, o teisėsaugos biudžetai yra pakankamai limituoti, teisėsaugai iškyla poreikis, kuo efektyviau panaudoti turimus resursus nusikalstamoms veikoms užkardyti ir išaiškinti (Casey, Burrell ir Sumner, 2019, p. 104). Algoritminės priemonės gebėdamos apdoroti didelius duomenų kiekius, suteikia naujų galimybių pagerinti rizikų aptikimo galimybes, supaprastinti tyrimo procesus ir sustiprinti prevencines priemones (Köbis et al., 2022; Lima & Delen, 2020; López-Iturriaga & Sanz, 2018; Sarker et al., 2023). Pasinaudodami algoritminių programų galimybėmis, teisėsaugos institucijos potencialiai gali padidinti atskaitomybę, skaidrumą ir sąžiningumą įvairiuose sektoriuose, galiausiai prisidėdami prie skaidresnės ir produktyvesnės valstybės kūrimo. **Antikorupcinės aplinkos gerinimas** – šiame darbe apibrėžiamas, kaip kompleksinis procesas, kuriuo siekiama sumažinti korupcijos rizikas optimizuojant viešojo sektoriaus veiklą, įskaitant skaidrumą, atskaitomybę ir atsparumą nesąžiningam elgesiui įvairiuose lygmenyse. Šis procesas apima ne tik teisėsaugos (pvz.: rizikų aptikimo, tyrimų optimizavimo aspektus), bet ir kitas sritis kaip: finansų sektorius (pvz.: pinigų plovimas su tikslu nuslėpti galimai korupciniais būdais gautą turtą), viešieji pirkimai, administraciniai sprendimai ir jų skaitmenizacija (pvz.: dokumentai lengviau atsekami, nėra galimybės modifikuoti ar manipuliuoti duomenimis).

Lietuvoje dirbtinio intelekto (toliau - DI) naudojimas aplamai yra nauja ir tik pastaruoju metu pritraukianti vis daugiau dėmesio tema. 2023 m. Transparency International atlikta studija, nurodo jog tik ¼ viešojo sektoriaus institucijų naudoja „algoritminius įrankius darbo našumui didinti, procesams optimizuoti, stebėsenai“ (Žemgulytė et al., 2023, p. 4). Tyrimų susijusių su šių priemonių pritaikymu antikorupcinės aplinkos gerinimui, Lietuvoje – nėra. Tačiau užsienio literatūroje yra daug pasižymėjusių mokslininkų, tiriančių DI naudą, žalą bei panaudojimo galimybes. Ne maža dalis mokslininkų, nurodo, DI naudą viešųjų pirkimų srityje (Adam & Fazekas, 2021, p. 3; Albert Sanchez-Graells, 2021, p. 3; Köbis et al., 2021, p. 7, 2022, p. 7; Odilla, 2023, p. 361; Per Aarvik, 2019, p. 1; Petheram et al., 2019, p. 8), tačiau verta pabrėžti, jog diskusijose apie šių technologijų naudą, tyrėjai akcentuoja ir potencialias šių technologijų grėsmes, tokias kaip: sistemų šališkumas, teisė į privatumą, atsakomybės už sprendimų priėmimą neaiškumas (Per Aarvik, 2019, p. 2), piktnaudžiavimas politine kontrole, siekiant pakenkti oponentams ar padėti sąjungininkams (Odilla, 2024, p. 28). Pabrėžiama specifinė rizika taikant algoritmus korupcijos aptikimui, kadangi šios technologijos apmokomos

teisisiais ir reguliavimo metodais, kurie orientuoti į formalius taisyklių pažeidimus (Ceva & Jiménez, 2022, p. 2), tačiau korupcija neapsiriboja vien formalių taisyklių pažeidimais, o taip pat šių technologijų naudojimas gali tapti įrankiu padėsiančiu korupcinėms veikoms vykti sparčiau (Adam & Fazekas, 2021, p. 3). Kelia žaloms užkirsti bei apsaugoti visuomenę, pasitelkiami ne tik švelniosios teisės (ang. soft law) ir švietimo metodai, tačiau ir naujas DI teisinis reguliavimas.

Šio darbo tikslas – ištirti algoritminių technologijų taikymą antikorupcijos srityje, analizuojant jų naudą, kylančius iššūkius ir potencialą, identifikuojant esamą įdirbi bei trukumus sukurti rekomendacijas efektyviai šių technologijų adaptacijai Lietuvoje.

Uždaviniai:

1. Remiantis mokslinė literatūra sukaupiti ir struktūruotai pateikti informaciją apie algoritmines technologijas ir jų valdysena, DI reguliavimo, potencialo ir žalos galimybes;
2. Surinkti ir išanalizuoti viešai prieinamą ES šalių informaciją apie algoritminių technologijų naudojimą antikorupcinei aplinkai stiprinti;
3. Atlikti interviu su DI srities mokslininkais bei specialistais, dirbančiais antikorupcinės aplinkos stiprinimo lauke, ištirti apie algoritminių įrankių taikymą šioje srityje, išryškinant esamą įdarbį, spragas, rizikas bei galimybes;
4. Suformuoti įrodymais grįstas rekomendacijas spartinančias DI ir jo gerųjų praktikų plėtrą stiprinant Lietuvos antikorupcinę aplinką.

Pasitelkiant dokumentų analizės metodą, surinkti viešai prieinami duomenys apie Europos Sąjungos (toliau - ES) šalių naudojamas sistemas įvairiose srityse, kurios padeda ne tik viešajame, bet ir privačiame sektoriuje stiprinti antikorupcinius metodus. Analizuotos 27 ES šalys, duomenų kaupimo bazei atrinkti 68 šaltiniai, o jų paieškai naudoti raktiniai žodžiai. Šie duomenys sukuria gerųjų praktikų sąrašą, kuriuo remiantis, daromos išvados apie sistemų veikimo sritis, funkcionalumą, pritaikomumą. Taip pat atliktas kokybinis tyrimas, t.y. interviu, su DI srities mokslininkais bei specialistais, dirbančiais antikorupcinės aplinkos stiprinimo lauke, suteikė informacijos pagrindą apie sėkmingai pritaikomas technologijas Lietuvoje, taip pat nurodė galimus pavojus bei kokios sąlygos yra būtinos efektyviam šių technologijų integravimui. Šio darbui uždaviniams atskleisti buvo atlikti 12 interviu (iš jų 2 grupiniai), juose dalyvavo 7 mokslininkai ir 9 specialistai.

Šio darbo struktūra: *literatūros apžvalga* – kurioje pateikiamas informacijos pagrindas apie algoritmines technologijas, jų valdysena, DI etikos principus, taip pat šių technologijų taikymo, darbui su korupcija, nauda ir žala bei DI akto esmė; *tyrimas ir diskusija* – kuriame atsakoma į empirinius darbo uždavinius bei pateikiamos viso darbo įžvalgos; bei darbo duomenimis grįstos – *išvados ir rekomendacijos*.

1. Algoritminių technologijų panaudojimas antikorupcinei aplinkai gerinti: norminis ir praktinis kontekstas

1.1 Algoritminių technologijų apibrėžimai

DI, mašininis mokymasis (toliau MM), blokų grandinės technologija (ang. Blockchain) ir kiti algoritmai dažnai vartojami lyg sinonimai, tačiau technologijų srityje, tai yra skirtingos sąvokos turinčios kertinių skirtumų savo funkcionalumu. Jų skirtumai paaiškina skirtingą sistemų taikymo sritį, galimą poveikį, naudą bei žalą, šios žinios taip pat svarbios kuriant jų valdymo ir priežiūros mechanizmus.

DI – tai „<...> sistemos, kurios demonstruoja protingą ir sumanų elgesį, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti“ (Europos taryba, 2018, p. 1). Panaši mintis buvo išreikšta UNICRI ir INTERPOL išleistoje, DI skirtos teisėsaugai, ataskaitoje, jog DI naudojami panašiais į žmogaus intelektą procesais: balso atpažinimas, kalbos vertimas, sprendimų priėmimas, problemų sprendimas ir to gali mokytis iš duomenų bazėse esančių dėsningumų, nereikalaujančių aiškių nurodymų iš žmogaus (UNICRI ir INTERPOL, 2020, p. 51).

MM yra DI pogrupis, kuriame daugiausia dėmesio skiriama algoritmų kūrimui, leidžiančių kompiuteriams mokytis iš duomenų ir laikui bėgant gerinti savo veiklą. MM – tai metodų, kurie sudaro dirbtinio intelekto pogrupį, algoritmai, kurie mokomi išvesti tam tikrą dėsningumą remiantis duomenų rinkiniu, tam kad nustatytų veiksmus reikalingus tikslui pasiekti (Europos komisija, 2020, p. 16). Literatūroje, taip pat pastebima, jog MM apibrėžimuose nebėra matyti žmogui prilygstančio arba pranokstančio intelekto charakteristikų.

Blokų grandinės technologija – tai decentralizuota skaitmeninė duomenų bazė, kurioje įrašai grupuojami ir susiejami kriptografiniu būdu, sudarant chronologinę nekintamų duomenų grandinę (Aarvik, 2020, p. 2). Skirtingai nei DI ar MM, kurie skirti daugiau duomenų analizei, blokų grandinės technologija nesimoko ir nepriima sprendimų, jos paskirtis yra užtikrinti duomenų nuoseklumą ir skaidrumą (Kayikci & Khoshgoftaar, 2024, p. 1).

Algoritmai – baigtinė griežtų instrukcijų seka, paprastai naudojama konkrečių problemų sprendimui arba skaičiavimams atlikti. Svarbu akcentuoti jog algoritmai yra pagrindinė DI ir MM metodų įgyvendinimo seka, kaip ir blokų grandinės technologijoje, tačiau kitu principu – joje atlieka saugumo vaidmenį (Per Aarvik, 2020), o DI/ MM mokymosi ar prognozavimo funkcijas.

Nors DI dažnai naudojama, kaip bendrinė sąvoka, apimanti įvairių tipų algoritmines technologijas, visų jų funkcionalumas skiriasi. MM – kaip DI pogrupis, orientuotas į didelių duomenų apdorojimą. Blokų grandinės technologija į dokumentų apsaugojimą, skaidrumo užtikrinimą. Tuo

tarpu algoritmai yra pagrindiniai šių sistemų kūrimo įrankiai, kuriuose pateikiamos skirtingo funkcionalumo algoritmų sekos. Visos šios sistemos tam tikra prasme susijusios arba gali būti susietos, tačiau išlieka svarbu akcentuoti jų skirtumus, norint veiksmingai jas naudoti tikslams pasiekti, tuo labiau – jas reguliuoti bei prižiūrėti.

1.2. Algoritminės valdysenos iššūkiai

Algoritminių technologijų integravimas į antikorupcinę veiklą suteikia reikšmingą poveikį teisės saugos srityje. Kadangi vyriausybės institucijos ir organizacijos visame pasaulyje stengiasi suvaldyti žalingą korupcijos poveikį bei jos plitimo mastą, DI ir kitais algoritmais remti įrankiai suteikia ne tik naujų galimybių optimizuoti teisės saugos veiklą, tačiau kelią ir didelių iššūkių, susijusių su duomenų valdymu, atskaitomybe ir teisiniu reguliavimu.

Dėl DI keliamų privatumo pažeidimų, duomenų šališkumo bei kitų rizikų, daugelis organizacijų, siekdamas užtikrinti patikimų sprendimų priėmimą, imasi duomenų valdymo (kuriuos naudoja, naudos sistemos, tai gali būti ne tik sutartys ar kito tipo administracinė informacija, bet ir individualių asmenų privatūs duomenys), kaip priemonės, leidžiančios kontroliuoti duomenų kokybę ir atitiktį atitinkamiems teisiniams ir etiniams reikalavimams spręsti (Janssen et al., 2020, p. 1). Algoritminę valdyseną galima apibrėžti, kaip tikimybę, jog specifinis sistemoje užkoduotų instrukcijų rinkinys galės priimti sprendimus be žmogaus įsikišimo ir/ arba struktūrizuoti galimą veiksmų lauką naudojant konkrečius duomenis (Issar & Aneesh, 2022, p. 3). Svarbu pabrėžti, jog šių technologijų naudojimas sukuria visai kitą terpę, kuri reikalauja tikslų procesų kontrolės mechanizmų bei daugiasluoksnių etikos principų. Akcentuojama, jog DI valdymas turėtų būti tarpvalstybinis požiūris siekiantis užkirsti kelią DI rizikoms atsirasti, bei praktika apimanti – organizacinę, teisinę, technologinę bei etinę pagrindą (Wirtz et al., 2022, p. 2). Tačiau netgi norint sukurti tinkamą DI teisinę pagrindą yra poreikis suprasti bei akcentuoti šių technologijų keliamas rizikas (Taeihagh, 2021, p. 138). Visgi literatūroje pabrėžiama, jog mūsų supratimas apie algoritmų keliamą riziką ir valdymą turi didelių spragų, o kuriant valdymo gaires dažnai neatsižvelgiama į konkretias DI rizikas (Wirtz et al., 2022).

Viešajam administravimui sunkiai sekasi žengti koją su sparčia DI raida – tai rodo konkrečių DI valdymo ir teisėkūros programų trūkumas, todėl politikos formuotojai turi spręsti su tuo susijusias grėsmes (W. Wirtz et al., 2020; Zuiderwijk et al., 2021, p. 3). Reaguojant į DI reguliavimo spragas, įstaigos ir vyriausybės priima savireguliacinio arba „švelniosios teisės“ (ang. Soft law) metodus, tokius kaip: standartus, gaires, elgesio kodeksus, kuria ekspertų komitetus rengiančius DI strategijas. Žinoma, gairės bei kiti tokio tipo įrankiai gali būti greičiau keičiami nei tradicinis teisinis reguliavimas, jos tampa pranašesnės siekiant neatsilikti nuo sparčios technologijų

raidos, tačiau šie metodai turi trūkumų užtikrinant įvairių suinteresuotųjų šalių įsitraukimą bei atstovavimą (Taeihagh, 2021, p. 145). Literatūroje galima rasti ir kritikos taškų šiam įsitraukimo procesui, kadangi būtent tai gali tapti klaidų atsiradimo šaltiniu, kai prie proceso prisijungia subjektai galintys pasinaudoti žinių pranašumu ir tuo, kad MM algoritmai daugumai institucijų vis dar yra nepakankamai suprantami (Taeihagh, 2021, p. 145), šiame procese taip pat gali atsirasti terpė korupcinėms rizikoms. Literatūroje nurodoma jog siekiant spręsti šias problemas, politikos formuotojai turi teikti pirmenybę įtraukiojo valdymo pobūdžiui sudarant sąlygas suinteresuotosioms šalims dalyvauti DI sistemų valdymo formavime. Tai reiškia, kad į procesą būtina įtraukti valstybines institucijas, nevyriausybines organizacijas ir visuomenės atstovus, siekiant užkirsti kelią šiuo metu pažangesnio, privačiojo sektoriaus įmonių lobistinei įtakai reglamentavimo procesams. Efektyviam DI valdymui labai svarbu pasiekti platų visuomenės sutarimą dėl DI etinių principų ir atskaitomybės mechanizmų (Wirtz et al., 2022), todėl platesnis skirtingų sričių įtraukimas padėtų pasiekti šių tikslų.

Verta akcentuoti ir tai jog dėl netolygaus algoritmų valdymo mechanizmo, bei taikomų „švelniosios teisės“ metodų, DI taikymo atsakomybės bei atskaitomybės aspektai dažnai tampa neaiškūs, o tai kenkia didžiųjų duomenų analizės sistemų (DDAS) duomenų kokybei ir tinkamumui naudoti (Janssen et al., 2020, p. 2). Dėl duomenų rinkiniuose esančios labai įvairaus formato informacijos (struktūrizuotos, pusiau struktūrizuotos ar nestruktūrizuotos) DDAS remiasi MM ir gilaus mokymosi metodais, o pastarajam, šiuo metu skiriamas didesnis dėmesys dėl jo specifinių funkcijų (Selmy et al., 2024, p. 1) (t.y. itin efektyvus didelių duomenų rinkinių apdorojimas). Daugelyje šaltinių vienas iš pirmųjų įstatymų, kuris yra minimas kalbant algoritminių programų tematika yra BDAR (Bendrasis duomenų apsaugos reglamentas) – tai Europos lygmens įstatymas, kuriuo yra nustatomos taisyklės susijusios su fizinių asmenų apsauga tvarkant jų duomenis bei laisvu asmens duomenų judėjimu (BDAR, 1str.). BDAR užtikrina asmenų teisę atsisakyti profiliavimo ir duomenų perdavimo, skatinant duomenų skaidrumą ir kontrolę, bei nurodo norminius ir technologinius reikalavimus, atitinkančius jos principus. Griežtos priemonės siekia užkirsti kelią tyčiniam duomenų piktnaudžiavimui, didinant algoritminio valdymo atskaitomybę formuojant jį taip, kad pirmenybė būtų teikiama duomenų apsaugai, naudotojų teisėms ir atsakingai duomenų tvarkymo praktikai (Europos parlamentas, 2020, p. 9). Tačiau literatūroje galima rasti BDAR įstatymo ribas bei išimtis, akcentuojama jog šiuo įstatymu nėra nuorodos į skirtingus gaunančiųjų subjektų gebėjimus suprasti algoritminių sprendimų reikšmę ir pasekmes (Taeihagh, 2021, p. 151). BDAR gali būti aiškinamas ir taikomas taip, kad netrukdytų DI naudotis asmens duomenimis ir nepadarytų ES įmonių mažiau konkurencingų nei ne ES konkurentų (Europos parlamentas, 2020, p. 7), o tai netiesiogiai nurodo jog šis reglamentas gali būti neefektyvus norint užkirsti kelią DI taikymo rizikoms. Taip pat BDAR nėra aiškiai paminėtas DI, yra minima tokie terminai kaip: internetas, socialiniai tinklai, nuorodos ir pan., dėl šių spragų gali kilti dviprasmybių norint remtis BDAR įstatymu, o DI kūrėjams

ir organizacijoms gali būti sunku suprasti, kaip tiksliai reglamentas taikomas jų technologijoms, todėl įstatymas gali būti taikomas nenuosekliai.

Svarbu pabrėžti, jog nei viena Europos sąjungos šalis neturi tiesioginio nacionalinio DI įstatymo, o jo veikla yra reguliuojama per kitus reglamentus bei teisės aktus: Pagrindinių teisių chartija, BDAR, Produktų atsakomybės direktyva, direktyvos dėl diskriminacijos, Vartotojų apsaugos teisės aktai ir kiti nacionalinio lygmens įstatymai. Literatūroje pabrėžiama, jog etiškas ir patikimas DI tam tikru mastu dažnai jau atsispindi galiojančiuose teisės aktuose, tačiau visiškas jo įgyvendinimas gali peržengti esamų teisinių įsipareigojimų ribas (Larsson, 2020, p. 444). Autorius remiasi argumentais jog didesnis ir specifiskesnis dėmesys šioms technologijoms turi būti taikomas dėl sparčios DI pažangos ir sudėtingo šių sistemų veikimo būdo. Kai kurios šalys, pasižymi požiūriu jog DI veikla neturėtų būti pertekliniai reguliuojama, kadangi prioritetu tampa laisvė inovacijoms, tačiau didelė rizika šiame kontekste siejasi su DI valdymo apimties ignoravimu ir svarbių valdymo aspektų praleidimu, kuris gali turėti neigiamų pasekmių (Wirtz et al., 2022, p. 10). Nors DI naudojimas valdžios institucijose gali padidinti piliečių pasitikėjimą, nes pagerina paslaugų teikimą, jis taip pat gali pakirsti pasitikėjimą dėl privatumo pažeidimų ir suvokiamo nesąžiningumo (Zuiderwijk et al., 2021, p. 10-14). Valdžios inertiškumo ir sparčios DI technologijų pažangos priešprieša dar labiau apsunkina valdymo iššūkius, todėl išryškėja specializuotų DI žinių poreikis vyriausybėse (Wirtz et al., 2022, p. 7).

Apibendrinus, nepaisant galimybių, kurias suteikia algoritminės programos, jos taip pat kelia naujų iššūkių, reikalaujančių tinkamo etinio ir teisinio pagrindo joms valdyti. Šiame procese svarbu užtikrinti visuomenės įtraukimą į procesų kūrimą ir bendrą sutarimą dėl etikos principų. Nors daugelis organizacijų priima savireguliacijos metodus siekdamos užtikrinti patikimą sprendimų priėmimą, literatūroje akcentuojamos ir jų spragos, esama didelių spragų supratime apie algoritmų sukeltą riziką ir tinkamą valdymą (ši dalis detaliau aptariama 1.3. skyriuje). Todėl svarbu toliau plėtoti žinias apie DI technologijų valdymą, kad būtų sukurta proporcinga ir efektyvi algoritmų valdysena.

1.3. DI etikos principai bei jų problematika

Kadangi DI sistemų naudojimas yra ganėtinai nauja tema, o teisinis jo veikimo reglamentavimas yra silpnas, principų joms sukūrimas bei įgyvendinimas gali užtikrinti saugumą bei teisingumą visuomenei. DI etikos principai yra tam tikros gairės, kuriomis turėtų vadovautis sistemų kūrėjai, prižiūrėtojai bei vartotojai visą jų gyvavimo ciklą, tam jog sistemos veiktų tinkamai. Šioje dalyje bus aptariami DI principai ir jų trūkumai iš kritinės perspektyvos.

Nors literatūroje principų rinkiniai yra skirtingos sudėties bei apimties tačiau, dažniausiai pasikartojantys principai išlieka: duomenų apsauga, atsakomybė ir atskaitomybė, skaidrumas, audito galimybė bei suinteresuotųjų šalių įtraukimas į DI procesus (UNESCO, 2021; Lyuben, A. et al. 2021; Ibarra, Douglas ir Tharmarajah, 2020; Berryhill et al., 2019; Jobin, Ienca ir Vayena, 2019). Tarptautinės organizacijos, tokios kaip JT, EBPO ir ES, taip pat nevyriausybinių organizacijų, bendradarbiaudamos su įvairiomis suinteresuotosiomis šalimis, rengia ir skatina DI etikos standartus (kuria ekspertų grupės), kad būtų užtikrintos išsamios gairės. Šie etiniai principai nebūtinai yra vieningi ir kartais gali prieštarauti vienas kitam. Derinant teisingumo ir žalos prevencijos vertybes gali kilti etinių dilemų, kai reikia atidžiai apsvarstyti kompromisus (European parliament, 2020, p. 87). Galima įžvelgti jog tam tikri DI etikos principai tampa, kai kurių principų įgyvendinimo dalimi (pvz.: proporcingumo ir žalos vengimo principo įgyvendinimas yra saugumo ir apsaugos principo užtikrinimo dalis). Taip pat matoma, jog tam tikri principai yra smarkiai susiję tarpusavyje, todėl įgyvendinant vieną privalu įgyvendinti ir kitą, tam kad principų sistema veiktų tinkamai (pvz.: nediskriminavimo principą vargu ar įgyvendintume neužtikrinę duomenų apsaugos ar skaidrumo).

2024 m. priimtame Europos tarybos DI akte yra nurodomi 7 DI etikos principai (kurie paremti dar 2019 m. DI ekspertų grupės nurodytais principais), kuriais turėtų remtis šių sistemų gyvavimas (žr. 1 pav.).

Etikos principas	Etikos principo reikšmė
Žmogiškasis veiksnumas ir priežiūra	DI sistemos turėtų tarnauti žmonėms, gerbti žmogaus orumą ir autonomiją, būti valdomos ir prižiūrimos žmogaus.
Techninis patikimumas ir sauga	Šios sistemos turėtų būti atsparios problemoms ir neleistiniams pakeitimams, kuo labiau mažinant nenumatytą žalą.
Privatumas ir duomenų valdymas	DI sistemos turėtų atitikti privatumo ir duomenų apsaugos taisykles, tvarkyti kokybiškus ir integralius duomenis.
Skaidrumas	Sistemos turėtų būti skaidrios ir paaiškinamos, informuojant naudotojus apie jų sąveiką su DI ir sistemos galimybes bei apribojimus.
Įvairovė, nediskriminavimas ir sąžiningumas	DI sistemos turėtų skatinti įvairovę, lygias galimybes, lyčių lygybę ir kultūrinę įvairovę, vengti diskriminacinio poveikio ir šališkumo.
Visuomenės ir aplinkos gerovė	Sistemos turėtų būti kuriamos ir naudojamos tvariai, teikiant naudą visiems asmenims ir stebint ilgalaikį poveikį visuomenei ir aplinkai.

1 pav. „Europos tarybos nurodomi DI etikos principai“

Akcentuojant Europos tarybos poziciją, etikos principai turėtų būti taikomi kuriant ir naudojant DI modelius. Šie principai turėtų būti pagrindas rengiant elgesio kodeksus pagal šį reglamentą, o suinteresuotosios šalys skatinamos įsitraukti į etikos principų kūrimą (Europos Sąjungos Taryba, 2024, p. 24-25). Svarbu pabrėžti, jog šiuose principuose nėra užtvirtinti atsakomybės bei atskaitomybės principai, kurie iš esmės turi vieną iš didžiausių įtakų teisėsaugos veikloje.

Vadovaujantis tik Europos tarybos pateikta DI etikos principų struktūra lieka neaiški atskaitomybės sistema, kuri kaip nurodoma, yra esminė norint užtikrinti sistemų stebėseną ir rizikų valdymą (Jamie Berryhill et al., 2019, p. 109). Taip pat nėra aiškiai apibrėžta, kas yra atsakingas (arba jog tai yra svarbu išsiaiškinti) už sprendimus, priimtus naudojant algoritmines technologijas.

Tačiau literatūroje atsiranda vis daugiau kritiškų pareiškimų, jog DI principai nors ir yra pamatinė sistema, kuria šiuo metu galima remtis, jiems trūksta konkretumo ir įgyvendinamumo, būtino veiksmingam valdymui. DI etikos iniciatyvose nesprendžiamos esminės normatyvinės ir politinės įtampos, susijusios su pagrindinėmis sąvokomis tokiomis, kaip teisingumas ar privatumas (Mittelstadt, 2019, p. 501), toks savireguliacinis etikos kodeksų laikymasis yra priežastis politikos formuotojams nesiimti naujo reguliavimo kūrimo (Calo, 2017, p. 409; Hagendorff, 2020, p. 100). Normatyvinė įtampa gali pasireikšti situacijose kai kyla konkurencija tarp vertybių, pvz. tarnyba kuria DI sistemą, skirtą stebėti viešųjų pirkimų procesą ir nustatyti galimus korupcijos atvejus. Problema gali kilti, kai tarnyba, neturinti aiškaus bei griežto reguliavimo DI sistemų kūrimo ir taikymo srityje (taikoma savireguliacija iš jau esamų tarptautinių organizacijų rekomendacijų), pasirenka sistemą, kuri greičiau demonstruoja rezultatus aptinkančius tik konkrečius korupcijos atvejus, tačiau praleidžiant subtilias jos formas. Pastarosios dėl savo sudėtingumo (fiktyvūs sandoriai, daugiasluoksniškumas ir pan.) ir latentiskumo gali likti visiškai nepastebėtos, nors būtent jos dažnai daro didžiausią žalą viešajam interesui. Čia aptariama savireguliacija gali ne tik nespręsti, tačiau ir padidinti politinę įtampą, pvz.: nesant aiškių įstatymų bei normų, o remiantis tik DI etikos principais bei rekomendacijoms, vyriausybė gali skatinanti naudoti DI sistemas viešųjų pirkimų stebėjimui, o paskirtos įmonės ar tarnybos pozicionuoti, jog naudojamos sistemos yra aukštos kokybės. Tačiau be išorinio spaudimo (aiškaus įstatymo numatytų normų laikymosi), tarnybos ar įmonės gali neatkreipti dėmesio į sistemos spragas pvz.: algoritmo šališkumo mažiau favorizuotų tiekėjų atžvilgiu.

Nurodoma, jog etikos principai dažnai tarnauja, kaip rinkodaros strategija nuraminti visuomenę ir dažnai daro labai mažą įtaką patiems sistemų kūrėjams, ji laikoma kaip tam tikra techninių problemų priedanga (Hagendorff, 2020, p. 112-114). Kol principai dažniausiai orientuoti į jautrių vertybių apsaugos užtikrinimą, didesnis dėmesys turi būti skiriamas galios centralizacijai ir socialinei nelygybei spręsti. Taip pat literatūroje atsiranda pastebėjimų jog DI etikos principai yra įtakojami vakarietiško (*ang. Western*) idėjų ir nors vakarų šalys atlieka svarbų vaidmenį kuriant ir tobulinant DI technologijas, tai gali būti netinkama ir nepritaikoma visoms visuomenėms (Segun, 2021, p. 99) (t.y. vakarų individualizmo poreikis atsispindintis DI etikos principuose gali būti nepritaikomas kolektyvistinių pažiūrų visuomenėms). Nors DI etikos gairės dažnai atrodo universalios (kadangi savyje talpina tokius principus, kaip: privatumas, teisingumas, paaiškinamumas), jų universalumas nebėra toks stiprus, kai pasižiūrime giliau į įvairias visuomenes, kuriose jis yra taikomas

(Hongladarom ir Bandasak, 2024, p. 2020). Nurodoma, jog yra tikslinga turėti platesnį etikos atstovavimą, kuris atsižvelgtų į įvairesnį etniškumą, be kurio gali pasireikšti parodymų neteisingumas (*ang. testimonial injustice*) (Segun, 2021, p. 99). Autorius nurodo jog parodymų neteisingumas suteikia mažesnį patikimumą teiginiui, pasiūlymui ar žinioms dėl išankstinių nuostatų apie asmens lytį, rasę, akcentą ir pan. Literatūroje, taip pat akcentuojama, jog DI etikos principai turi atliepti platesnį socialinį ir ekologinį kontekstą, kuriame veikia DI bei raginama pereiti prie labiau įtraukiančio ir tarpdisciplininio, socio-techninio požiūrio į DI etiką (Hagendorff, 2022, p. 501-508).

Apibendrinant, galima išskirti ir tai, jog mokslininkai daugiausia akcentuoja tai, kaip galima patobulinti DI etikos principus, tam jog jie pasiektų didžiausią savo, kaip įrankio, potencialą. Nors literatūroje randama DI etikos principų kritikos yra svarbu pabrėžti jog tai yra politikos formuotojų, technologų ir kitų suinteresuotųjų šalių orientyrai, skatinantys kolektyvinę atskaitomybę, atsakomybę, platesnį visuomenės įsitraukimą, informuotumą bei kontrolę (Mittelstadt, 2019, p. 504), o kritiškas požiūris ir nepasitikėjimas gali padėti neignoruoti rizikų bei efektyviai į jas reaguoti (Hagendorff, 2022, p. 862). Mokslinėje literatūroje nėra atmetamas DI etikos principų reikalingumas, anaip tol etikos principai yra nurodomas, kaip geras orientyras bei įrankis, kuriuo gali remtis ne tik asmenys dirbantys su šiomis technologijomis, tačiau ir technologijų kūrėjai, bei politikos formuotojai. Svarbu pabrėžti, jog tai yra tik pagalbinė priemonė, teisingo bei naudingo, DI kūrimo procese.

1.4. Galima algoritminių įrankių naudojimo nauda korupcijos srityje

Teisingas algoritminių priemonių ir DI naudojimas kovojant su korupcija teikia daug žadančių galimybių. Nurodoma, jog „Sėkmingiausia, kai DI priemonės įtraukiamos į esamus procesus ir papildo esamas kovos su korupcija pastangas, o ne visiškai jas pakeičia“ (Guillaume Nicaise ir Daniel Sejerøe Hausenkamph, 2025). Tinkamai naudojamos algoritminės technologijos gali padidinti skaidrumą, sumažinti žmogiškąjį šališkumą ir padidinti korupcinės veiklos nustatymo veiksmingumą. Šioje dalyje, remiantis įvairiais moksliniais tyrimais, nagrinėjama galima algoritminių priemonių nauda efektyvinant darbą su korupcija.

Kadangi autorių, nagrinėjančių antikorupcijai taikomų algoritminių sistemų nėra daug, šiame – naudos, bei kitame – žalos, skyriuose buvo pasitelktas mišrus informacijos sintetinio metodo. Apibendrinta informacija ir analizuojami autorių darbai, kurie tiesiogiai susieti su DI taikymo nauda bei galima rizika ir žala antikorupcijos srityje, taip pat į analizę įtrauktos ir autorių nuomonės apie DI taikymo teisėsaugoje (aplamai) privalumus bei trūkumus, o vėliau šios įžvalgos sugretintos su korupcijos prevencijos bei antikorupcinės aplinkos stiprinimo procesais.

Algoritminės priemonės geba veiksmingai apdoroti didelius duomenų rinkinius (Adam ir Fazekas, 2021, p. 7-7) ir nustatyti įtartina veiklą, pvz., neįprastus finansinius sandorius ir viešųjų pirkimų anomalijas, interesų konfliktus (Odilla, 2023), analizuojant viešojo sektoriaus duomenis galima aptikti sąsajų, kurios gali rodyti korupcijos riziką. Tai padidina institucijų gebėjimą stebėti operacijas realiuoju laiku ir atskleisti paslėptus modelius, kurių žmonės gali nepastebėti (Adam & Fazekas, 2021; Fazekas, 2017; Wirtz & Müller, 2019). Automatizavus šiuos procesus, tampa įmanoma padidinti korupcijos aptikimo greitį, ir tikslumą. DI tam tikrus procesus padaro veiksmingesnius ir kokybiškesnius (Wirtz, Weyerer ir Geyer, 2019, p. 596; Europos veiksmingo teisingumo komisija, 2018, p. 65). Literatūroje nurodoma, kad DI programų veikla gali palengvinti ir pagreitinti veiklos sritis geriau paskirstant teisėsaugos išteklius, gali efektyviau nustatyti dėsningumus milžiniškuose duomenų rinkiniuose (Meijer ir Wessels, 2019, p. 1031 – 1133; Casey, Burrell ir Sumner, 2019, p. 104; Ibarra, Douglas ir Tharmarajah, 2020, p. 23), kurių analizė rankiniu būdu užtruktų daug ilgiau ir tikėtina atneštų mažiau naudos.

MM grindžiamų programų taikymas baudžiamųjų veikų tyrimuose suteikia galimybę atlikti auditą, nuoseklumo ir kontrolės bei veiklos stebėseną (Ibarra, Douglas ir Tharmarajah, 2020, p. 23), kas skatina sistemų tobulinimą bei visuomenės pasitikėjimą jomis. Kita algoritminė sistema galinti padėti šioje srityje yra blokų grandinės technologija – jos pagalba duomenys įrašomi chronologiškai, užtikrinant saugumą ir atsparumą klastojimui (Kayikci & Khoshgoftaar, 2024, p. ; Per Aarvik, 2020, p. 12). Skirtingai nei tradicinės duomenų bazės, į blokų grandinės technologija remtą sistemą galima tik pridėti informaciją, todėl ji tampa patikimu sandorių ir duomenų sekimo įrankiu (Kayikci & Khoshgoftaar, 2024). Atsižvelgiant į tai, jog korupcinio pobūdžio veikų tyrimai užtrunka ilgai, tyrimai susideda iš didelio kiekio procesinių veiksmų bei dažnu atveju būna itin sudėtingi, audito bei stebėsenos galimybė tampa aktuali, norint už(si)tikrinti, jog visi veiksmai tyrime buvo padaryti tinkamai ir nepažeidžiant tam tikrų normų – tuo pačiu užtikrinant skaidrumo principą. Taip pat tai gali tapti neatsiejama viešųjų paslaugų proceso dalimi, pvz.: viešieji pirkimai, kur sutarčių stebėseną ir duomenų atsekamumas, stebėjimas bei tyrimas yra vieni iš pagrindinių rizikos nustatymų šaltinių.

Atsižvelgiant ir į tai jog specialistai dirbantys teisėsaugos srityje susiduria su dideliais darbo krūviais, ilgomis procedūromis, darbuotojų ar ekspertų trūkumu, biurokratizmo kliūtimis, kurios neretu atveju sukelia rutininio darbo jausmą (Wirtz & Müller, 2019), šio pobūdžio sistemos padėtų ne tik supaprastinti kasdienes užduotis, bet leistų specialistams daugiau laiko skirti darbui, kuris suteikia didesnę vidinę pasitenkinimą. Antikorupcijos sritis ne išimtis, darbuotojai dažnai susiduria su įvairių dokumentų šabloniniu pildymu ar procedūriniais darbo niuansais, kurie užima laiko, tačiau nesuteikia pridėtinės vertės jiems, kaip specialistams naudoti ar tobulinti profesines žinias.

Esamos DI technologijos dažnai naudojamos, kaip prognozuojančios sistemos (Odilla, 2023, p. 359), kurios siekia užkirsti kelią korupcijai stebėdamos signalus ir aptikdamos galimai įtartinus veiksmus prieš faktinį pažeidimą. Algoritminės sistemos geba efektyviai prognozuoti korupcinio pobūdžio veikas, remiantis praeitais korupcijos atvejais. MM modeliai, paremti istoriniais duomenimis, gali identifikuoti sritis, kuriose yra didesnė korupcijos rizika dar prieš įvykstant pažeidimams (Aldana et al., p. 3, 2022; Rabuzin ir Modrušan, 2019, p. 335). Šis funkcionalumas leidžia optimaliai nukreipti išteklius į tas sritis ar sektorius, kuriuose korupcijos tikimybė yra didžiausia, taip prisidedant prie efektyvesnio korupcijos valdymo. Ši algoritminių programų nauda leidžia imtis prevencinių priemonių (Köbis et al., 2021; Poltoratskaia & Fazekas, 2024), kuriomis tvarkomos bei šalinamos esamos spragos didelės rizikos srityse.

Algoritminės priemonės gali sumažinti žmogiškąjį šališkumą pateikdamos duomenimis pagrįstą analizę ir sprendimus, o tai sumažina žmogaus subjektyvumą nustatant ir sprendžiant korupcijos atvejus. Žmogiškasis šališkumas gali būti susijęs su kultūriniais, socialiniais ar politiniais veiksniais (Odilla, 2023; Pagano et al., 2023). Pavyzdžiui, tinkamai sukurtos, DI valdomos sistemos gali objektyviai analizuoti duomenis ir teikti rekomendacijas, taip nedarant įtakos subjektyviam (pvz. specialisto) vertinimui, kurie kartais gali pakenkti tradiciniams darbo su korupcija metodams, pvz. subjektyvumas gali atsirasti nuo asmens matomos medijos ar turimų ryšių ar/ir socialinio rato. Be to, DI priemonės didina skaidrumą sumažindamos žmogaus valdomų manipuliacijų tikimybę (Parycek et al., 2024, p. 8405; 8415), pvz. automatizuodamos viešųjų pirkimų procesų ir kitų biurokratinių funkcijų stebėseną. Taip skatinamas viešojo administravimo teisingumas ir mažinama konkrečių grupių diskriminacija, jeigu sistemų duomenys yra tinkami, o pačios priemonės naudojamos teisingai.

Tinkamai sukurtos bei naudojamos DI grindžiamos sistemos, gali užtikrinti procesų skaidrumą leidžiant realiuoju laiku stebėti viešųjų pirkimų procesus, padaro duomenis prieinamus bei gali užtikrinti, kad įvairūs subjektai laikytųsi numatytų taisyklių. Ši priemonė riboja galimybes nesąžiningai veiklai, pro-aktyvus požiūris gali užkirsti kelią korupcinės veiklos plitimui (Köbis et al., 2021). Puikus to pavyzdys yra Estija, kurios „e.vyriausybės“ sistema turi „X-Road“ platformą, kurios pagalba atsiranda galimybė realiuoju laiku stebėti viešuosius pirkimus, saugiai keistis duomenimis bei suteikia galimybę visiems stebėti bei pranešti apie įtartinas veikas, taip mažinant korupcijos riziką (Dobrovolska & Rozhkova, 2024, p. 232). Verta akcentuoti ir tai jog 2021 m. ES Pranešėjų apsaugos direktyva įpareigojo visas nares įgyvendinti šifruotas platformas, kuriomis asmenys galėtų pranešti apie korupciją ar sukčiavimą. Būtent tokie įrankiai gali padidinti pranešimų skaičių, išsaugant jų privatumą ir anonimiškumą, bei sudaryti sąlygas visuomenei aktyviau prisidėti prie korupcijos ir sukčiavimo šalinimo (Adam & Fazekas, 2021, p. 9; Dobrovolska & Rozhkova, 2024, p. 233; Jenkins et al., 2022, p. 14).

Korupcijos kontekste dažnai pastebimas nebaudžiamumas, ypač tarp valdžią turinčių asmenų (Odilla, 2023). Verta pabrėžti, jog valstybės tarnautojai neretai piktnaudžiauja diskrecijos teise viešajame sektoriuje, o politikai, kaip pažymi tyrėjai, sąmoningai siekia sukurti diskrecijos galimybes, kad galėtų manipuliuoti procesais ir siekti asmeninės naudos (Adobor & Yawson, 2022, p. 3; Parycek et al., 2024). Verta akcentuoti ir tokius reiškinius, kaip „institucinė korupcija“ (ang. *Institutional corruption*) (Lessig, 2013) arba „teisinė korupcija“ (ang. *Legal corruption*) (Dincer & Johnston, 2020), kurie palieka teisines spragas, naudojamas savanaudiškais tikslais. Teisėta korupcija – orientuota į iš esmės legalius, tačiau neetiškus veiksmus, pvz. asmuo, iš pažinčių struktūroje sužino apie specifinės žemės pabrangimą dėl ten planuojamų pokyčių, dar prieš tai, kol tai taps žinoma ir tuo pasinaudojęs nusiperka tą žemę. Institucinė korupcija – daugiau orientuota į sisteminės, struktūrinės spragas ir jų pasinaudojimu asmeninei naudai. Šiame kontekste, algoritminės sistemos galėtų sumažintų galimybes asmenims manipuliuoti duomenis ir informacija jiems naudingais tikslais bei prisidėtų prie didesnio skaidrumą viešajame sektoriuje.

DI sistemos gali padėti supaprastinti tarpvalstybinius korupcijos tyrimus, nes sukuria erdvę lengvesnei duomenų dalybai, kurią galima įdarbinti naudojant tas pačias ar panašaus tipo sistemas (GDR insight, 2021, p. 241). Sukurti ir priimti atviri DI standartai padėtų bendradarbiauti tarpusavyje (UNESCO, 2021, p. 23), o tai palengvintų įvairių šalių ir institucijų bendradarbiavimą bei korupcijos prevenciją aplamai, kuri dažnai susijusi su sudėtinga tarptautine veikla. Informacijos skaida gali pagerinti ne tik tarptautinius bendradarbiavimo santykius, bet turėti įtakos ir kasdienėje, visuomenės vartojamoje, medijoje. DI paremtos sistemos gali būti naudojamos, kaip priemonės, nukreiptos į piliečių ugdymą, siekiant šviesti visuomenę arba diegti vyriausybės politiką, subtiliais, bet tikslingais veiksmais (Wirtz & Müller, 2019, p. 11). Wirtz ir Müller nurodo, kad toks įrankis gali tapti ne tik nešančiu gerą, bet galingu įrankiu formuojant politinę kontrolę ir piliečių elgesį. Medijoje skleidžiama informacija turi reikšmingą poveikį visuomenės formavimui apie vykstančius politinius procesus, o tai gali formuoti nuomonę ne tik teisėkūros srityje (pvz. „čekiukų“ skandalo įtaką siūlymui pakeisti LR BK 228 str. (Piktnaudžiavimas), bet ir visuomenės požiūryje į aplamai korupciją. Tai gali rodyti skirtingus DI sistemų polius, tačiau specifiskam tikslui, kokybiškai pritaikytos sistemos gali atnešti pilietiškumo bei antikorpucinio švietimo naudos skleidamos pozityviai nukreipiančią informaciją medijoje.

Apibendrinant, algoritminės priemonės ir DI sistemos suteikia reikšmingų galimybių kovojant su korupcija. Šios technologijos padeda automatizuoti viešojo sektoriaus procesus, identifikuoti korupcijos rizikas, o pro-aktyvūs sprendimai prisideda prie didesnio skaidrumo ir efektyvesnių kontrolės mechanizmų. DI leidžia analizuoti didžiulius duomenų kiekius, aptikti anomalijas, kurios gali rodyti korupcijos požymius ir realiuoju laiku stebėti viešųjų pirkimų bei finansinius procesus,

sumažinti žmogaus manipuliacijų galimybes. Nepaisant šių privalumų, DI grindžiamos kovos su korupcija priemonės vis dar turi būti tobulinamos, kad būtų galima sušvelninti tokius iššūkius, kaip duomenų kokybės problemos, algoritmų šališkumas ir etinės problemos ir pan. Tačiau sprendžiant silpnąsias vietas bei kokybiškai pritaikius algoritmines priemones, tai tampa daug žadantis įrankis kontrolės valdymui gerinti ir korupcijos galimybėms mažinti.

1.5. Galima algoritminių įrankių naudojimo žala korupcijos srityje

Daugelis DI antikorupcinių technologijų yra palyginti naujos, o ilgalaikiai jų poveikio tyrimai tebėra riboti (Guillaume Nicaise ir Daniel Sejerøe Hausenkamph, 2025, p. 4), jų taikymas gali kelti rimtų iššūkių ir grėsmių teisėsaugai, teisėkūrai, politikos formuotojams bei plačiajai visuomenei. Nors šie įrankiai gali padėti identifikuoti galimas nusikalstamos veikos rizikas ir padidinti viešųjų ir privačiųjų procedūrų skaidrumą, jie taip pat gali įtvirtinti šališkumą, skatinti neteisingus sprendimus ir dėl jų veikimo spragų sukelti neigiamų pasekmių. Dėl šių priežasčių, sprendimų priėmėjams, svarbu ne tik efektyviai naudoti algoritminius įrankius, bet ir užtikrinti jų etiškumą bei atsparumą netinkamam jų naudojimui. Šiame skyriuje bus aptarti algoritminių įrankių galimos žalos, naudojant juos antikorupcinės aplinkos kūrimo.

Šališkumas reiškia sisteminį palankumą arba išankstinį nusistatymą tam tikrų asmenų ar grupių atžvilgiu, kuris gali pasireikšti įvairiuose DI programos naudojimo etapuose: renkant klasifikatorius, mokant modelius, klaidingai interpretuojant rezultatus, kuriant požymius (Odilla, 2023, p. 358). Šališkumo iššūkiai, MM įrankiuose, nuodugniai tyrinėjami, atsižvelgiant ne tik į teisę, verslo praktiką, visuomenės tradicijas, tačiau ir į etinius apribojimus (Pagano et al., 2023, p. 2). Atsižvelgiant į tai, kad nesąžiningumo samprata skiriasi tarp kultūrų, o skirtingos duomenų bazės lemia nenuoseklius rezultatus (Odilla, 2023, p. 359), šališkumo mažinimas tampa sudėtingu procesu, kuris reikšmingai apsunkina praktikos standartizavimo galimybes įvairiuose kontekstuose. Dėl atsirandančio duomenų šališkumo sprendimų priėmėjai gali neteisingai interpretuoti duomenis ir priimti netinkamą sprendimą, ypač tokiose jautriose srityse, kaip baudžiamoji justicija ir viešasis administravimas. DI sistemose nesąžiningumas gali kilti dėl triukšmo (ang. *Noice*) (Szreder, 2022). Triukšmas reiškia atsitiktinius ar nepageidaujamus nukrypimus, kurie daugiausiai atsiranda duomenų rinkimo ar apdorojimo metu, pavyzdžiui, dėl to panašios korupcinio pobūdžio bylos gali būti traktuojamos nevienodai. Nurodoma, jog sistemų nesąžiningumas taip pat gali kilti dėl netinkamo DI technologijų taikymo (Szreder, 2022, p. 48), pvz. kai specialistai per daug pasitiki DI sistemų sprendimais ir jų nekvestionuoja.

Mokslininkai atkreipia dėmesį į tai jog antikorupcinės technologijos sukurtos ir apmokytos nustatyti riziką daugiausiai remiasi teisiniais ir reguliavimo metodais, kurie dažnai orientuoti į formalius taisyklių pažeidimus (Ceva ir Jiménez, 2022, p. 2), tačiau verta pabrėžti, kad korupcija neapsiriboja vien aiškiais formalių taisyklių ar reglamentų pažeidimais. Taip pat literatūroje akcentuojama ir tai jog tam tikros korupcinės praktikos yra moraliai ginčytinos tačiau ne visos visuotinai priimanamos, kaip neteisėtomis (Odilla, 2023, p. 359). Egzistuoja neetiškos praktikos, kurios išnaudoja teisinių sistemų spragas bei trūkumus, tačiau formaliai neatlieka teisės pažeidimo. Galime paminėti anksčiau aprašytus reiškinius „teisėta korupcija“ ir „institucinė korupcija“, kurie kol kas sunkiai aktualizuojami kalbant apie duomenų realybės atspindėjimą. Šie reiškiniai, dėl savo specifinės bei sudėtingos išraiškos sunkiai apdorojami į duomenis, kurie gali būti naudojami algoritminėse sistemose, todėl neatliepiant šių reiškinių, gali būti sudėtinga užtikrinti duomenų realybę ir šios veikos gali likti latentinės.

Mokslinėje literatūroje keliama klausimai susiję su nepakankamu algoritminių technologijų skaidrumu ir atskaitomybės trūkumu, o korupcijos srityje šios spragos gali tapti itin žalingos. Dėl šių trūkumų DI priemonės gali veikti kaip „juodosios dėžės“ (ang. *black box*) (Ceva & Jiménez, 2022; Odilla, 2024; Per Aarvik, 2019; Wirtz & Müller, 2019), kai jų procesai ir sprendimų priėmimo kriterijai yra neaiškūs arba painūs, todėl jas sunku įvertinti ar užtikrinti atsakomybę bei atskaitomybę – o tai, kaip minėta ankstesnėse šio darbo dalyse, išlieka itin svarbu. „Juodosios dėžės“ efektas, duomenų netinkamumas ir panašūs aspektai, sudaro prielaidas manipuliacijoms ir piktnaudžiavimui, ypač korumpuotoje aplinkoje (t.y. aplinkoje, kurioje naudojamosi esamomis procesų spragomis, o korupcijos reiškinys normalizuojamas, kaip būdas pasiekti tikslų), kurioje sisteminiai trūkumai gali būti lengvai išnaudojami. Turint omenyje šią algoritminių technologijų spragą, gaunami rezultatai gali būti sunkiai paaiškinami bei atsekami pagal pradinius įvesties duomenis, o suinteresuoti asmenys gali manipuliuoti kodu ir (arba) mokymo duomenimis siekdami asmeninės naudos (Jenkins et al., 2022, p. 10). Tokius atvejus aptikti taptų ypač sudėtinga, todėl sistemų projektavimo etape itin svarbu, kad praktikai būtų supažindinti su sistemoje nustatytais reikšmėmis ir jų charakteristikomis (Coalition For Integrity, 2021, p. 45; Kossow et al., 2021, p. 16). Jenkins ir kt., taip pat pateikia pavyzdį, kai vaizdo klasifikavimo algoritmai gali būti lengvai manipuluojami, o tai sudaro galimybes sveikatos priežiūros darbuotojams įsitraukti į korupcinę veiklą, siekiant neteisėtai padidinti išmokas iš draudimo ir pan. Galima papildyti, jog toks sistemų manipuliavimas, gali sudominti farmacijos industriją, kuri bandytų papirkti sveikatos priežiūros specialistus su tikslu gauti daugiau pelno.

Literatūroje galima rasti ir tyrimų, kuriuose nurodoma, jog algoritminės technologijos veiksmingiausiai padėjo dirbti su žemo lygio ar smulkiaja korupcija, o jų poveikis didžiajai korupcijai dažnai buvo nereikšmingas dėl elito ar turinčių galią nesuinteresuotumo spręsti sisteminės korupcijos

problema (Adam & Fazekas, 2021, p. 3). Akcentuojant korupcinio pobūdžio nusikalstamas veikas ir tai jog šios veikos siejamos su baltųjų apykaklių nusikaltimais (ang. *White collar crimes*), galime teigti, jog institucijų naudojamos algoritminės sistemos, gali tapti įrankiu, padėsiančiu šioms veikoms vykti sparčiau (Adam ir Fazekas, 2021, p. 11; Köbis et al., 2021, p. 7, 18, 2022, p. 6-7). Nurodoma jog ypatingai silpnos teisinės valstybės sąlygomis DI pagrindu vykdomos antikorupcinės kampanijos dažnai tampa valdžios įrankiu politiniams oponentams slopinti, o valdžią turintys asmenys gali naudotis šiomis sistemomis kad stiprinti galios struktūra tokiu būdu didinant piktnaudžiavimą valdžia riziką ir socialinę nelygybę (Köbis et al., 2022).

Teigiama, jog DI gali tapti valdymo priemone, įrankiu stebėti ir kontroliuoti žmones, o šios sistemos dažnai patenka į visuomenės grupių rankas turinčias galią (Hagendorff, 2022, p. 852). Naudojant DI, kyla privatumo ir masinio stebėjimo pavojus, kadangi sistemos gali realiuoju laiku rinkti ir analizuoti duomenis, tokius kaip privačių medijose esančių anketų informacija arba rinkti korupcijai nagrinėti svarbius duomenis pvz. nuolatinis finansinių srautų stebėjimas. Tai leistų valdžios institucijoms nuolat stebėti piliečių elgesį, o surinkti duomenys gali tapti piktnaudžiavimo taikiniu (Wirtz & Müller, 2019). Nurodoma, jog vyriausybės naudoja šias sistemas žurnalistams, politikams ir jų oponentams stebėti (Jenkins et al., 2022, p. 9), o tai gali pažeisti tokius etikos principus, kaip privatumas, kai sistemos yra naudojamos neproporcingai (nors ir siekiant antikorupcinės aplinkos gerinimo tikslų). Taip pat galima pabrėžti ir kitą šių technologijų nesąžiningumo pusę, kai jos gali būti naudojamos politinės valdžios atstovų, kurie piktnaudžiauja valstybės tarnyba ir mokėdami už mikrotikslines reklamos kompanijas medijose, manipuliuoja rinkėjų pasirinkimą savo partijos naudai (Jenkins et al., 2022, p. 9). Akcentuojant šią pusę, politinių partijų finansavimas bei jų protegavimas medijose, gali sukurti naujų korupcijos formų bei iššūkių norint nustatyti pažeidimus šioje srityje.

Plėtojant paskutiniąją mintį, egzistuoja galimybė jog algoritminės priemonės gali sudaryti sąlygas korupcijos skatinimui bei naujoms jos formoms atsirasti (Adam & Fazekas, 2021), o tai žinoma, gali sumažinti visuomenės pasitikėjimą teisėsauga bei skatinti piktnaudžiavimą korumpuotoje aplinkoje. Literatūroje randama tyrimų, kurie nurodo, kad kai DI patarimai suderinami su asmenine nauda, žmonės jais pasitiki, o tai indikuoja, kad DI gali tapti nauja priemone korupcijai skatinti, sumažindamas moralinį barjerą ir padarydamas nesąžiningą elgesį lengviau pateisinamą (Leib et al., 2021, p. 11-12). Tai reiškia jog specialistas gali priimti šališko DI sistemos rezultatus, jeigu tai būtų naudinga jam, pvz. sistema patvirtintų jo turimą subjektyvią nuomonę apie specifinio asmens galimai daromas korupcines veikas. Svarbu pabrėžti ir tai, jog korupcinių veikų vykdymas per DI sistemas dažnai lemia atsakomybės sklaidą, nes šių veikų atveju atsakomybės difuzija mažina tiek jų aptikimo, tiek sankcijų taikymo tikimybę, o neteisėto elgesio kontekste asmenys linkę perkelti

kalbę kitiems (NTIA, 2024; Jenkins et al., 2022, p. 10). Visa tai referuoja į neutralizacijų taikymą nusimetant atsakomybę nuo sprendimų priėmėjo, o tai žinoma gali vesti ne tik į neskaidrius procesus, bet ir neteisingus rezultatus antikorupcinėje veikloje.

Jei algoritmai nėra kruopščiai suprojektuoti, jie gali sustiprinti esamas galios struktūras. Būdingas šališkumas gali sietis su skirtingais duomenų rinkimo metodais, policijos praktikomis, lokacijos ir laiko aspektu, istoriniais įvykiais ar tam tikros grupės susidomėjimu (Ibarra, Douglas ir Tharmarajah, 2020, p. 11). Pažymima, jog algoritminės sistemos yra tiek geros, kiek geri yra joms pateikti duomenys, tačiau jei korumpuoti veikėjai manipuliuoja įvestais duomenimis, jie gali išvengti aptikimo (Dobrovolska & Rozhkova, 2024, p. 234). Kiekvienas iš nurodytų aspektų gali lemti tam tikrų grupių prioretizavimą, pvz., jei duomenys renkami tam tikroje vietovėje arba tam tikru laikotarpiu, tai gali sukurti neproporcingą atstovavimą tam tikroms grupėms ar įvykiams, taip iškreipiant duomenų rezultatus. Žinoma, nereikia atmesti galimybės, jog asmenys programuodami algoritmus, gali perkelti savo šališkumus bei vertybes, taip sustiprinant stereotipus bei diskriminaciją (Wirtz, Weyerer ir Geyer, 2019, p. 605). Jei sistemos teikia pirmenybę tam tikroms nuomonėms ar visuomeninėms hierarchijoms, jos gali padidinti nelygybę, ypač jei taikomos korumpuotoje aplinkoje, kur esamos socialinės ir politinės struktūros yra pažeistos.

Kibernetinių atakų metu, užpuolikai gali įgauti prieigą ne tik prie žmogaus fizinės gyvenamosios vietos duomenų, bet ir prie jo kriminalinės istorijos (Wirtz & Müller, 2019, p. 603), kuri vėliau gali būti panaudota šantažui, bei kitų nusikalstamų veikų efektyvumo didinimui. Žinoma, teisėsaugos institucijos dirbančios su itin jautria ar slaptumo žymas turinčia informacija, suformavo tvirtą procedūrą, apsaugančią šiuos duomenis nuo viešumo ar kitokio duomenų nutekėjimo. Tačiau yra svarbu pažymėti, jog netinkamai veikiantys algoritmai, bei turinčios spragų programinės įrangos gali tapti silpnąja grandimi, bei turėti pasekmių ne tik specifiniams asmenims, tačiau ir valstybės ekonomikai ar net nacionaliniam saugumui. Literatūroje pateikiami pavyzdžiai, kai įvairių kibernetinių atakų metu, įsilaužimai į strategiškai svarbių įmonių ar institucijų sistemas, lėmė didelio masto duomenų vagystes, kurios sukėlė rimtą susirūpinimą dėl jų skaitmeninės infrastruktūros saugumo (Dobrovolska & Rozhkova, 2024, p. 233-234).

Apibendrinant, netinkamai sukonstruoti ir apmokyti algoritmai gali sustiprinti esamą šališkumą ir skatinti neteisingus/ neteisėtus sprendimus. Algoritmų „juodosios dėžės“ specifika bei duomenų šališkumas kelia iššūkių sprendimų atskaitomumui bei etiškumui, o tai ypač pavojinga korumpuotoje aplinkoje, kur tokios priemonės gali būti lengvai išnaudotos. Šiuolaikinėje literatūroje pabrėžiamas nepakankamas DI priemonių skaidrumas, galintis lemti visuomenės pasitikėjimo mažėjimą. Taip pat algoritminių technologijų naudojimas gali sukelti pavojų asmens duomenų privatumui bei skatinti jo

pažeidimus bei manipuliacijas medijose, o šią terpę gali išnaudoti neskaidrios struktūros bei galios valdytojai.

1.6. DI aktas – struktūra ir problematika

2024 m. Europos Parlamentas išleido Europos Sąjungos DI aktą (toliau - aktas), kuriuo siekiama užtikrinti nuoseklią ir aukšto lygio apsaugą bei išvengti vidaus rinkos susiskaldymo (dėl nevienodų esamų nacionalinių taisyklių), ES šiuo reglamentu nustato vienodą teisinę sistemą DI technologijų kūrimui, pateikimui rinkai ir naudojimui, taip skatindama į žmogų orientuotą ir patikimą DI įsisavinimą bei inovacijų plėtrą (Europos Parlamentas, 2024/1689). Tai yra pirmasis tarptautinio lygmens teisinis dokumentas, kuriuo turi vadovautis visos sąjungos narės. Taip pat svarbu paminėti 2023 m. ISO „Informacinės technologijos – Dirbtinis intelektas – Valdymo sistema“ standarto vaidmenį– „ISO/IEC 42001 parengtas siekiant reaguoti į skubius klausimus, susijusius su nekontroliuojama DI plėtra ir galimomis grėsmėmis“ (ISO, 2024). Šiame skyriuje bus aptariamai esminiai DI sistemų reguliavimo ypatumai.

DI akte, sistemoms nustatyti reikalavimai yra paremti rizikos kiekio kontrolės būdu, reglamente yra nurodomi 4 rizikos lygiai: nepriimtina rizika, aukšta rizika, ribota rizika (sistemos su specifine skaidrumo prievole) ir minimali rizika. **Nepriimtinos rizikos sistemos** yra nurodomos, kaip sistemos, kurios sukurtos: manipuliacijos tikslais, pažeidžiamumų išnaudojimui, socialiniui vertinimui (ang. Social scoring), asmenų nusikalstamo elgesio prognozavimui, masiniui duomenų rinkimui veidų atpažinimo tikslais, emocijų atpažinimui darbo vietose ir mokyklose, biometriniai profiliavimui, veido atpažinimui viešose vietose teisėsaugos tikslais. Nors pagal aktą šios sistemos yra draudžiamos, visgi joms taikomos tam tikros išlygos, pvz. socialinis vertinimas draudžiamas tik tuo atveju, jei dėl to atsiranda žalingas ar nepalankus elgesys socialiniame kontekste, kuris nesusijęs su kontekstu, kuriame duomenys buvo iš pradžių surinkti, arba yra nepagrįstas ar neproporcingas (DI aktas, 5 str. 1d. c punktas). Turint omenyje, kad socialinio vertinimo sistemos patenka į nepriimtinos rizikos kategoriją ir tai, jog aktas nustato ribas, kad jos tampa nepriminamomis tik atsiradus žalai, palieka ne mažą terpę manipuliuoti suteikta šios sistemos naudojimo galia. Taip pat išlygos taikomos ir teisėsaugos valdomoms veido atpažinimo sistemoms viešose vietose. Šios sistemos gali būti taikomos siekiant: atlikti tikslinę aukų paiešką, užkirsti kelią konkrečiai ir neišvengiamai (terorizmo) grėsmei arba nustatyti asmens, kuris yra nuteistas arba (net tik) įtariamas padaręs konkretų sunkų nusikaltimą, buvimo vietą ar tapatybę (DI aktas, 5 str. 1d. h punktas). Mokslinėje literatūroje nurodoma, jog šio tipo kameros vėliau gali būti naudojamos nuotolinio biometrinio identifikavimo tikslais, jei tenkinamos išskirtinės aplinkybės, taip išplečiant funkcijų išplitimo ir piktnaudžiavimo teisėsaugos įgaliojimais galimybes (Sandra Wachter, 2024, p. 678; Nathalie A. Smuha, 2025, p. 237).

Aptariant **Aukštos rizikos sistemas**, kurios būtų aktualios šio darbo rėmuose (iš viso nurodomos 8 sistemų kategorijos), akte įvardijamos sistemos: lemiančios galimybes gauti svarbiausias paslaugas; biometriniam identifikavimui, emocijų atpažinimui ir profiliavimui; teisėsaugos srityje, darantis poveikį pagrindinėms teisėms (pvz., įrodymų vertinimas); migracijos ir sienų kontrolės srityje (pvz., automatinis vizų tvarkymas); teisingumo ir demokratijos srityje (pvz., teismo sprendimų rengimas). Literatūroje nurodoma, net jei jų sistema yra įtraukta į aukščiau išvardintas kategorijas, DI teikėjai gali patys įvertinti, ar jų sistema tikrai kelia riziką „sveikatai, saugai ar pagrindinėms teisėms“, ir tik tada jiems taikomi aukštos rizikos reikalavimai (Nathalie A. Smuha, 2025, p. 238). Žinoma, akte, nuo 8 iki 15 straipsnių yra išdėstomi sistemų atitikties reikalavimai, o 16-17 straipsniai nurodo, jog sistemų tiekėjai, kūrėjai turi adaptuoti tai ir pritaikyti technologijai. Iš tiesų, aktas kelia daug klausimų, tokių kaip: ar šių sistemų paslaugų tiekėjai yra pakankamai legitimūs, jog galėtų tinkamai įvertinti sistemų riziką ypač, kai jie nebus rizikos subjektai ir galimai nepatirs galimos žalos (Nathalie A. Smuha, 2025, p. 241-242). Mokslinėje literatūroje nurodoma, jog akte yra dviprasmybių, tam tikros straipsnių dalys gali būti suprantamos taip, jog į riziką, kurios neįmanoma sumažinti kuriant sistemas, galima neatsižvelgti, nors taip pat kitose dalyse galima interpretuoti ir taip jog tokią riziką turinčios DI sistemos neturėtų būti leidžiamos į rinką (Nathalie A. Smuha, 2025, p. 242). Svarbu akcentuoti, jog kategorijose trūksta tokių svarbių sričių, kaip medijos, mokslas, finansai, draudimas ir pan, kuriose naudojami DI įrankiai gali kelti didelę riziką visuomenei (Sandra Wachter, 2024, p. 682). Taip pat nurodoma, jog nustatytos aukštos rizikos sistemų nekoreguotinos kategorijos (tik kategorijoje esantis sistemų sąrašas gali būti papildomas) gali būti linkusios į per didelio arba nepakankamo įtraukimo problemas (Nathalie A. Smuha, 2025, p. 242), o tokiu būdu į rinką gali patekti nesureguliuotos rizikos sistemos. Taip pat pabrėžiama, jog akto 27 str. nurodyta viešosios teisės reglamentuojamoms bei viešąsias paslaugas teikiančioms įstaigoms privaloma atlikti „poveikio pagrindinėms teisėms vertinimą“ prieš pradedant naudoti sistemą – tai bus galima atlikti naudojant automatizuotą priemonę. Tai kelia riziką, jog šis prevencinis mechanizmas taps tik formaliu procesu neatsižvelgiant į esminę šio mechanizmo prasmę. Taigi, šių sistemų reguliavimas, iš esmės atitenka į kūrėjų, diegėjų rankas, o pats akto pritaikymas turintis daug neaiškumų, sukuria įvaizdį, jog akto įgyvendinimas priklausys nuo specialistų vertinimo.

Ribota rizika apibrėžiama akto 50 str., juo nurodoma, kad DI sistemoms gali kilti specifinė rizika, kaip: apsimetinėjimas arba apgaulė (į šią kategoriją įeina: *ang. Chatbots, Deepfakes* ir pan.), kuri skiriasi nuo didelės rizikos sistemų, tačiau gali būti priskiriamos ir prie aukštos rizikos sistemų. Šioms sistemoms taikomos papildomos skaidrumo visuomenei prievolės, tam jog būtų išvengta žalos, tačiau mokslinėje literatūroje nurodoma, jog tai gali būti nepakankamas mechanizmas norint išvengti galimos žalos (Sandra Wachter, 2024, p. 684).

Visos kitos DI sistemos, kurios nepatenka į vieną iš pirmiau minėtų rizikos kategorijų yra laikomos nerizikingomis arba turinčiomis **minimalią riziką** ir joms neprivalomi akto teisiniai įpareigojimai – kūrėjai juos gali taikyti pasirinktinai (Sandra Wachter, 2024, p. 684).

Šioje vietoje svarbu akcentuoti tarptautinį ISO standartą. Šis įrankis yra aptartų sistemų trečiosios šalies auditu (ISO, 2024), t.y. papildomas procesas, kurio metu yra tikrinama sistemos kokybė bei atitiktis su aktu, kitais susijusiais reglamentais bei etikos principais. Šiuo mechanizmu sistema įgautų sertifikatą, kaip įrodymą, jog sistema atitinka visus esamus reikalavimus bei yra tinkamai naudojama. Atsižvelgiant į tai, jog pagal aktą sistemos kūrėjai, o vėliau ir diegėjai turi įvertinti sistemos rizikos lygį, ISO sertifikavimas taptų trečiuoju sistemos tikrinimo etapu, todėl kyla klausimas ar visi šie procesai gali veikti harmoningai rinkoje, vykdant efektyvią DI grėsmių prevenciją? Kiek tai turės įtakos inovacijų plėtrai? Iš ties, atliepiant jau anksčiau minėtas, mokslinių darbų mintis, apie procesų tapimą tik formalumu, svarbu šią įžvalgą pabrėžti ir čia. Nors šį standartą šalys gali taikyti savanoriškai, kyla klausimas ar Lietuvoje sertifikuota sistema nesukels kitų šalių perteklinio pasitikėjimo, nepaisant to, kad sistema, tinkama vienoje šalyje, tačiau gali būtų žalinga kitoje.

Apibendrinant, šių reguliacinių mechanizmų atsiradimas ne tik nurodo atsiradusį suinteresuotumą, jog šios technologijos ne tik būtų taikomos tinkamai, tačiau suinteresuotumas matomas ir jų taikymo apimtyje. Kaip matyti, išlieka daug neaiškumų bei galimų interpretacijų įvairiuose DI sistemų kūrimo, diegimo, naudojimo etapuose, tačiau svarbu pabrėžti, jog teisinio dokumento – akto atsiradimas yra didelis žingsnis link skaidresnio bei žmogaus teisių apsaugančio (lyginant su aukščiau minėtais švelniosios teisės metodais) DI panaudojimo tiek viešajame, tiek privačiajame sektoriuose.

2. Algoritmai antikorupcinei aplinkai gerinti: dviejų pakopų metodas

2.1. Tyrimo metodika

Norint suprasti, kaip DI technologijos gali prisidėti prie efektyvesnės antikorupcinės aplinkos kūrimo, reikia išsamaus tyrimo, apimančio ne tik esančią literatūrą šia tematika, tačiau ir realias specialistų patirtis. Darbo 2-am bei 3-iam uždaviniui išpildyti buvo taikomi du skirtingi metodai: dokumentų analizė ir kokybinis tyrimo metodas – pusiau struktūruoti interviu. Dokumentų analizė atlikta su tikslu norint susisteminti naudojamas algoritmines technologijas temos srityje. Interviu atliekami su dviem tiriamųjų grupėmis, pirmoji – mokslininkai, antroji – specialistai, kurių darbo rezultatai prisideda prie antikorupcinės aplinkos gerinimo. Naudojant pusiau struktūruotą interviu

metodą buvo nagrinėjama jų patirtis, DI priemonių veiksmingumas, įgyvendinimo iššūkiai, etiniai aspektai ir reikšmingo poveikio pavyzdžiai. Taigi, šių dviejų metodų derinimas leido užtikrinti, kad tyrimas apimtų tiek teorinį, tiek praktinį požiūrį, formuluojant išsamius ir pagrįstus atsakymus į darbo uždavinius. Informacija gauta iš skirtingų profesinių kampų suteikė lyginamosios naudos ir padėjo išskirti aiškius probleminius temos aspektus.

Dokumentų analizė: antrasis uždavinys yra sutelkti informaciją apie Europos Sąjungoje taikomas algoritmines sistemas, kurios skirtos stiprinti skaidrumą, spartinti anomalijų aptikimą ir/ ar analizuoti informaciją korupcijos prevencijos srityje. Europos sąjungos šalys pasirinktos dėl bendro, joms taikomo teisinio reglamentavimo (mintyje turima ES 2024 m. DI aktą, bei kitus taikomus/ naudojamus standartus, principus bei rekomendacijas).

Siekiant užtikrinti duomenų patikimumą pasitelkta įvairaus tipo medžiaga: tarptautinių organizacijų dokumentai, ES bei šalių registrai, teisėsaugos institucijų bei organizacijų pranešimai, mokslinė literatūra, nacionaliniai šalių dokumentai, bei kitos susijusios viešai prieinamos publikacijos (remtasi 68-iomis publikacijomis, nurodyta 2 priede). Verta paminėti jog į šią analizę buvo įtraukti ir susijusių algoritminių technologijų implementavimo projektai, kurie vis dar procese arba tik pradedami vykdyti. Aktualumui užtikrinti buvo naudojami konkretūs raktiniai žodžiai: „*Artificial intelligence*“, „*Machine learning*“, „*Deep learning*“, „*Language learning models*“, „*Algorithms for corruption*“, „*Algorithmic technology used by anticorruption agencies*“ – šalia nurodant šalį. Taip pat, technologijų paieškai spartinti buvo pasitelkti papildomi imties kriterijai susiję su sistemų funkcionalumu (žr. 2 pav). Sistemų funkcionalumas buvo kategorizuojamas atsižvelgiant į mokslinės literatūros analizės metu akcentuojamas sistemų galimybes.

Funkcija	Paiškinimas
Aptikimas ir stebėjimas	Korupcijos požymiams finansiniuose sandoriuose, viešųjų pirkimų procesuose, teikiant viešąsias paslaugas.
Rizikos vertinimas	Analizuoja didelius duomenų kiekius, kad įvertinti kylančią riziką skirtinguose sektoriuose, procesuose, bei padėtų nustatyti anomalijas bei galimos korupcijos ar piktnaudžiavimo apraiškas.
Tyrimų palengvinimas	Automatizuojant duomenų analizę, spartinant biurokracinius ir administracinius procesus.
Atitiktis (ang. compliance) ir deramas patikrinimas (ang. due diligence)	Gali padėti organizacijoms užtikrinti, kad būtų laikomasi kovos su korupcija taisyklių, stebint, kaip laikomasi vidaus politikos, atliekant verslo partnerių patikrinimus ir pažymint galimus interesų konfliktus.
Skaidrumas ir atskaitomybė	Palengvina skaidrumo iniciatyvas, nes pagerina prieigą prie duomenų, apdoroja vyriausybės dokumentus ir stebi viešąsias procedūras, taip skatindamos didesnę atskaitomybę ir priežiūrą.
Viešųjų paslaugų teikimas	Didina viešųjų paslaugų teikimo efektyvumą, nes optimizuoja išteklių paskirstymą, mažina biurokratinės kliūtis ir didina piliečių įsitraukimą, taip mažindami korupcijos galimybes, nes

2 pav. Sistemų atskyrimas atsižvelgiant į skirtingą technologijų funkcionalumą bei paskirtį

Duomenys t.y. naudojamų technologijų sąrašai, pagal šalis, buvo sugretinami, palyginami tarpusavyje ir apibendrinami. Sistemų bei technologijų lentelėje buvo pildomos sritys: šalis, algoritmo tipas, sistemos funkcija bei šaltinis. Duomenų analizė atlikta naudojant „Microsoft Excel“ programinę įrangą, kuri leido apdoroti tyrimui surinktus duomenis, siekiant užtikrinti tikslų ir struktūruotą rezultatų pateikimą. Taipogi, tyrime įtrauktos visos ES šalys, dėl jų geografinės padėties bei konteksto, leido atskleisti bendras inovatyvumo tendencijas algoritminių technologijų taikyme antikorupcinei aplinkai gerinti ([šalių sąrašas](#)). Lyginamoji analizė padėjo identifikuoti pažangias praktikas ir skirtumus tarp šalių, sudarant tinkamą pagrindą rekomendacijoms bei teikiant vertingą informaciją apie gerąsias praktikas politikos formuotojams bei teisėsaugos institucijoms. Svarbu pabrėžti, jog šio uždavinio rezultatai papildė ir pusiau struktūruotuose interviu gaunamus atsakymus, padėdami geriau nustatyti tiriamųjų žinias apie kitų šalių pažangą DI technologijų taikymo srityje.

Interviu: trečiasis uždavinys yra ištirti, kaip algoritminės technologijos gali būti naudingos antikorupcinės aplinkos gerinimui, bei remiantis specialistų bei mokslinės bendruomenės atstovų nuomone nustatyti šių technologijų pritaikymą, naudojimą bei kylančius iššūkius. Šiam tikslo pasiekimui pasirinkta kokybinė tyrimo prieiga dėl siekio giliau suprasti tiriamųjų pusių poziciją bei išsamiai nagrinėti DI taikymo praktikos niuansus tarp mokslininkų/ teoretikų bei specialistų patirčių. Kokybiniai tyrimai leidžia analizuoti tiriamą objektą kompleksiskai, vertinant ne tik faktinius duomenis, bet ir ekspertines tiriamųjų patirtis. Tokio tyrimo metodo taikymas suteikia galimybę aptarti sudėtingus ir mažiau struktūruotus klausimus, kurie gali būti sunkiai paaiškinami kiekybiškai. Remiantis šiuo pagrindimu buvo atliekami pusiau struktūruoti interviu, gairės sudarytos atsižvelgiant į skirtingas tiriamųjų grupes (žr. *1 priedas*). Šiam uždaviniui išpildyti buvo išsikelti atraminiai klausimai:

1. Kokie yra praktiniai algoritminių technologijų naudojimo būdai ir jų vertinimas?
2. Kokie iššūkiai gali kilti/ kyla taikant algoritmines technologijas šioje srityje?
3. Koks yra DI etikos principų vaidmuo bei DI reguliavimo praktika mokslinės bendruomenės ir specialistų požiūriais?
4. Kokios šių technologijų taikymo galimybės darbui su skaidrumu viešuosiuose procesuose, anomalijų aptikimu bei efektyvesniu korupcinio pobūdžio veikų tyrimu?

Mokslinės bendruomenės atstovai, šiame tyrime, yra atrinkti, atsižvelgiant į jų mokslinę sritį, į ją patenka mokslininkai dirbantys su DI tema iš teisės, socialinių mokslų, informacinių technologijų pusės. Specialistai atrinkti per profesinį susietumą su tema bei atsižvelgiant į jų praktinę patirtį –

asmenys dirbantys su DI grįstomis technologijomis, dirbantys su korupcinės aplinkos gerinimo sritimi, asmenys įsitraukę į DI proceso, gairių bei visuotinės informacijos kūrimą. Abiejų tiriamųjų grupių atstovų rinkimas buvo grindžiamas sniego gniūžtės metodu. Šių dviejų grupių pasirinkimas pagrįstas siekiu gauti kuo išsamesnę ir objektyvesnę informaciją apie tiriamą temą iš skirtingų požiūrio kampų (žiūrėti pav. 3). Grupių pasirinkimą taip pat lėmė mokslinėje literatūroje akcentuojama teorijos ir praktikos atskirtis – teisiniai ir etiniai DI aspektai nuolat kinta, o praktikoje jų įgyvendinimas vis dar kelia iššūkių.

Grupė	Tiriamųjų darbinė sritis	Interviu tipas	Tiriamųjų skaičius	Interviu laikas
Mokslinė bendruomenė	Teisės, socialinių mokslų, informacinių technologijų mokslininkai nagrinėjantys DI temą	Individualūs, pusiau struktūruoti interviu	7	Nuo 25 m. 30 s. iki 58 m. 02 s.
Specialistai	Specialistai susiję su viešaisiais pirkimais, finansų priežiūra, antikorupcijos ir skaidrumo stiprinimo sritimis	Individualūs, pusiau struktūruoti interviu	3	Vidurkis - 34 m. 9 s.
		Du grupiniai, pusiau struktūruoti interviu	6	

3 pav. Informacija apie tiriamuosius bei interviu

Iš viso buvo atlikti 12 nuotolinių interviu su 16 asmenų, naudojant „Microsoft Teams“ ir „Zoom“ platformas. Du iš jų buvo grupiniai interviu inicijuoti pačių teisėsaugos institucijų specialistų. Interviu įrašyti naudojant „OBS Studio“ įrankį, o transkribuoti naudojant „SonixAI“, „Auscis“, „Transkriptor“ programas. Duomenys analizuojami pasitelkiant MAXQDA programinę įrangą. Vykdamas kokybinę turinio analizę bei siekiant nustatyti bendras temas ir unikalias išvalgas pritaikytas kodų ir subkodų medis (1 priedas). Analizės metu mokslininkų citatos žymimos – M1, M2..., specialistų citatos žymimos – S1, S2...

Tyrimo ribotumai. DI ir algoritminių priemonių taikymas teisėsaugos srityje ypač antikorupcinės aplinkos kūrimui yra sudėtinga tema ir iš dalies gali būti apribota dėl informacijos prieigos. Daugelis teisėsaugos institucijų priemonių nėra skelbiami viešai, dėl operacinės saugos bei poreikio apsaugoti jautrią informaciją. Dėl to prieiga prie šios informacijos tampa ribota ne tik visuomenei bet ir tyrėjams. Svarbu pabrėžti ir tai jog ši sritis yra gana nauja ir specifinė, daugelyje kitų šalių naudojamos sistemos taip pat nėra viešai prieinamos ar išsamiai aprašytos viešojoje erdvėje. Tai reiškia, kad nemaža dalis kitų šalių antikorupcinių DI priemonių, nepaisant jų inovatyvumo ir veiksmingumo, lieka uždaros akademinei ir visuomeninei.

Papildomą iššūkį gali sukelti ir tai jog Lietuvoje nėra mokslininkų, kurie orientuotųsi būtent į DI technologijų taikymą antikorupcinės aplinkos gerinimo kontekste. Lietuvos mokslininkų bendruomenėje ši tema yra mažai atstovaujama, daugiausiai dėmesio skiriama šių technologijų

taikymui plačiąja prasme tiek viešajame sektoriuje tiek privačiame, gerinant kasdienius veiklos procesus. Tačiau svarbu atkreipti dėmesį jog nevertėtų sumažinti tyrimo legitimumo, kadangi struktūruotuose interviu klausimai pritaikyti atskleisti DI būdingus iššūkius, etinius ar teisinius aspektus aktualius tiriant šios srities praktinį pritaikymą.

Etika. Tyrimo metu buvo vadovaujamasi pagrindiniais tyrimų etikos principais, siekiant užtikrinti dalyvių teises bei apsaugoti jų privatumą. Vienas svarbiausių tyrimo principų yra konfidencialumo užtikrinimas, kuris apsaugo tiriamųjų asmenų tapatybę bei jų pateiktą informaciją (Žydrūnaitė ir Sabaliauskas, 2017, p. 341). Konfidencialumas buvo užtikrintas laikantis griežtos informacijos apsaugos politikos, t.y. interviu duomenys buvo prieinami tik tyrėjui bei magistro baigiamojo darbo vadovei. Kadangi tyrime dalyvavo jautrių sričių specialistai, buvo imtasi priemonių, kad tyrimo rezultatuose nebūtų pateikiama asmenis identifiukuoti galinti informacija. Tai reiškia, jog interviu analizėje nebuvo pateikiamos darbo vietos, pareigos, konkrečių situacijų ar įvykių, kurie galėtų tiesiogiai ar netiesiogiai identifiukuoti tiriamąjį asmenį. Taip pat darbe teisėsaugos institucijų pavadinimai neviešinami dėl tikslo padidinti dalyvavimo tikimybę bei užtikrinti anonimiškumą. Taip pat tyrimo metu buvo vadovaujamasi savanoriškumo ir informuoto sutikimo principais. Prieš pradėdant interviu, kiekvienam dalyviui buvo pateikta išsami informacija apie tyrimo tikslus, procedūrą bei jų teisę atsisakyti dalyvauti bet kuriuo metu. Dalyviai buvo aiškiai informuoti, kad tyrime surinkta informacija bus naudojama tik šiam akademiniam darbui ir nebus viešai prieinami, išskyrus apibendrintus duomenis. Tiriamieji taip pat buvo informuoti jog interviu metu gali pranešti apie paminėta per daug jautrią informaciją, kuri neturėtų atsispindėti darbe. Galiausiai, surinkti įrašai po atliktos analizės buvo sunaikinti, siekiant užtikrinti kad jokia informacija negalėtų patekti į pašalines rankas ir nebūtų panaudota ateityje.

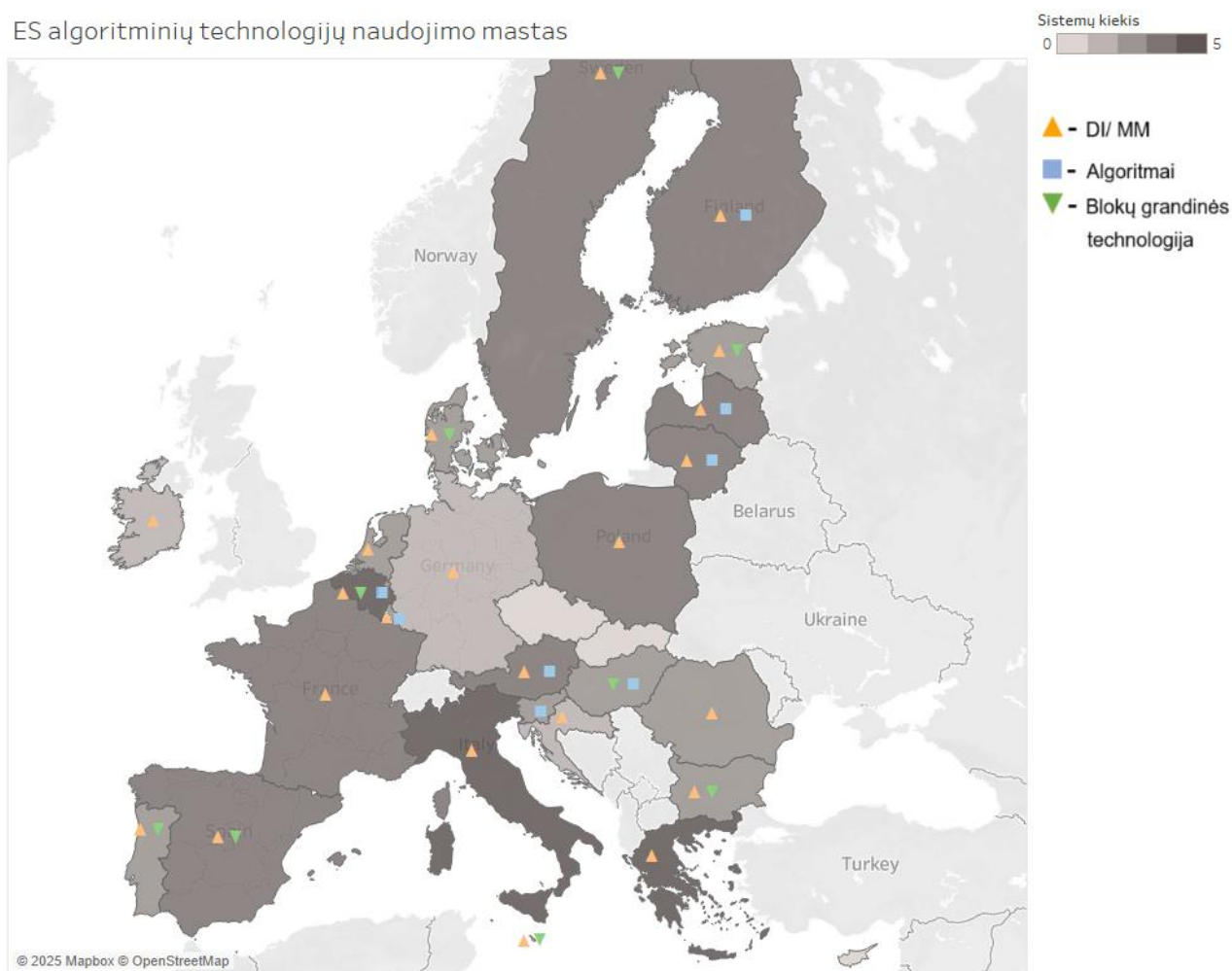
2.2. Dokumentų analizė: ES šalių algoritmų technologijos antikorupcinės aplinkos gerinimo veikloje

Algoritminės technologijos – tokios kaip, DI, MM, blokų grandinės technologija bei kiti pažangūs algoritmai – vis dažniau yra įdarbinami didinant skaidrumą, efektyvinant viešąsias paslaugas ir darbui su korupcija. Šioje dalyje bus analizuojamos visų ES šalių viešai prieinama informacija bei skelbiamos naujienos apie algoritminių technologijų pritaikymą antikorupcinei aplinkai gerinti. Analizės metu bus nurodomi bendri dėsningumai, šalių išskirtinumas, kritika, taip pat šių technologijų potenciali įtaka nelegalaus elgesio aptikimui.

Pažymėtina, jog dėl itin ribotos viešai prieinamos informacijos tampa sudėtinga tiksliai įvardinti, kokio tipo algoritmai yra naudojami nurodomose sistemose, ypač tais atvejais kai ta pati

sistema (pvz.: „VATcalc“, „Arachne“) gali turėti kelias versijas, kurios turi skirtingų funkcijų bei varijuojančių algoritmų ar net versijas, kuriose įvesta paprastoji analitika neturinti savyje algoritminių kodų. Atsižvelgiant į tai, analizėje įtrauktos tik tos sistemos, kurios įvardina arba dalinai suteikta galimybė daryti išvadą apie tai, kokia algoritmų rūšis yra naudojama.

Iš surinktų duomenų, matoma, jog didžiausią technologijų kiekį naudoja Belgija, Italija, Graikija (žr. pav. 4), Čekija, Kipras bei Slovakija neturėjo viešai prieinamų duomenų apie tyrimo rėmuose naudojamas technologijas, kitų šalių sistemų kiekis dažniausiai varijuoja tarp 2-3, tačiau pagrindiniai dėsningumai bei išskirtinimai atsiskleidžia analizuojant sistemų tipą, paskirtį bei funkcionalumą.



Pav. 4 „ES algoritminių technologijų naudojimo mastas“

Didžioji dalis rastų sistemų yra taikomos viešųjų pirkimų duomenų analizei efektyvinti (žr. 1 lentelę ir 2 priedą „ES šalių algoritminių technologijų naudojimas antikorupcinei aplinkai gerinti“). Beveik visos ES šalys taiko sistemas įvairiuose viešųjų pirkimų etapuose tam jog būtų aptinkamos riziką keliančios sutartys, pasiūlymai ar bendrąja prasme rizika keliantis dalyvaujančių subjektų elgesys.

DI/ MM	Belgija, Graikija, Ispanija, Italija, Kroatija, Rumunija, Latvija, Lietuva, Lenkija, Prancūzija, Suomija, Švedija, Vengrija.
Blokų grandinės technologija	Belgija, Bulgarija, Danija, Estija, Ispanija, Malta, Portugalija
Paprastieji algoritmai	Belgija, Liuksemburgas, Slovėnija, Suomija

1 lentelė „Algoritminės technologijos viešiesiems pirkimams ES“

Pagal rastą informaciją, Italija bei Prancūzija, išsiskiria naudojamų technologijų tikslingumu bei apimtimi. Italija taiko DI/ MM įrankius viešųjų pirkimų procesuose – po konkursų vykdo duomenų analizę, siekdama nustatyti galimus ryšius tarp perkančiųjų organizacijų ir privačių įmonių, bei stebėti ar sandoris vykdomas tinkamai. Taip pat eksperimentuoja su galimybėmis stebėti ir sekti vartotojus viešojoje erdvėje analizuojant jų reakciją į konkursus. Tuo tarpu Prancūzija naudoja DI/MM gristą sistemą „Anticor“, kuri lygina tikėtiną ir faktinę konkurso dalyvių elgseną, kad pažymėtų sutartis, kuriose yra didelė korupcijos tikimybė (tikrina interesų konfliktus, favoritizmą, suklustotas sutartis ir pan.), o Graikija dalyvaudama „Falcon“ projekte orientuojasi į stambiosios korupcijos aptikimą (fiksuoja politinius interesų konfliktus, sukčiavimo atvejus) viešuosiuose pirkimuose – toks sistemų įdarbinimas leidžia patikrinti didelį kiekį konkursų, net ir neturint daug žmogiškųjų resursų. Prancūzija taip pat pasitelkia DI įrankius, kurie sieja palydovinių vaizdų duomenis apie asmenų vartojimą, t.y. mašinos, baseinai ir pan. pobūdžio objektai, kurie indikuoja apie nepagrįstai padidėjusias asmens pajamas. Belgijoje taikoma „MEDIAAN“ platforma, leidžia stebėti ir analizuoti istorinius viešųjų pirkimų kainų duomenis, o ši informacija gali nurodyti tam tikras rizikas ar neskaidrius sandorius. Taip pat Belgija viešai paskelbė, jog taiko algoritmus paskirstant vaikus į mokyklas, o tai panaikina smulkiosios korupcijos – neoficialių susitarimų riziką. Lenkija pasižymi sistema „ETNA“, kuri skirta veiksmingai tvarkyti, apdoroti ir vertinti piliečių pranešimus apie galimus korupcijos atvejus, tai yra vienintelė rasta tokio pobūdžio sistema ES.

Taip pat pastebima tendencija naudojant blokų grandinės technologiją – šalys šią technologiją naudoja siekiant automatizuoti viešųjų pirkimų konkursus, taip pat išmaniųjų sutarčių sudarymui ar tam tikros informacijos registravimui. Jos funkcionalumas leidžia padidinti skaidrumą bei užkirsti kelią duomenų manipuliacijai, kadangi užfiksuoti duomenys blokų grandinės technologijoje negali būti modifikuojami, todėl informacija tampa patikimesnė bei lengviau atsekama bei tikrinama. Belgija išsiskirianti naudojamų algoritmų įvairove bei plačiu blokų grandinės technologijos naudojimu, kartu su agentūros „Digipolis“ pagalba, kuria viešųjų pirkimų platformos prototipą, gristą blokų grandine. Ši sistema leis paskelbti, pateikti bei atverti pasiūlymus decentralizuotame registre, manoma, jog tai užtikrins kiekvieno viešojo pirkimo etapo patikimumą. Šie viešai skelbiami

duomenys parodo tikslingą bei sisteminę taktiką įdarbinant algoritmines technologijas skaidrumui bei nelegalaus elgesio rizikų aptikimui skirtingose srityse, bei viešųjų paslaugų etapuose. Panašius pilotinius projektus vykdo Portugalija bei Malta, siekiant automatizuoti viešųjų pirkimų sutarčių sudarymą naudojant išmaniąsias sutartis – tai ne tik sumažintų rankinio darbo, bet ir panaikintų duomenų manipuliacijos galimybes, nes sutartys blokų grandinėje taptų nekintamos bei lengviau audituojamos. Tuo tarpu Estija jau ilgą laiką taiko „KSI Blockchain“ technologiją savo valstybinių duomenų registrų vientisumui užtikrinti, tai ne tik prisideda prie skaidrumo, tačiau kaip minėta teorinėje dalyje – blokų grandinės technologija gali papildyti DI, suteikdama geros kokybės duomenis sistemų apmokymui ir palaikymui.

Iš 2 priede pateiktų duomenų tik Austrija, Vokietija, Airija bei Nyderlandai, neturėjo viešos informacijos apie taikomas algoritmines technologijas viešųjų pirkimų srityje. Tačiau Austrija, Vokietija, Airija bei kita didelė dalis ES šalių taiko įvairaus tipo algoritmų sistemas PVM bei kitų mokesčių sukčiavimo aptikimams ar pajamų ir turto analizei, o tai itin sietina su korupcinio pobūdžio veikomis, kai asmenys aktyviai stengiasi nuslėpti turimą ar įgytą turtą. Švedija naudoja DI/ MM grįstą sistemą skirtą užtikrinti skaidrų naujų įmonių kūrimą analizuojant mokesčių mokėjimo vengimo rizikas. Prancūzija naudoja DI, kad automatiškai pastebėtų anomalijas ar taktikas, atitinkančias PVM vengimo, nedeklaruotų pajamų ar kitokio sukčiavimo požymius. Portugalija įdarbina DI/ MM priemonę palengvinančią keitimąsi elektroninėmis apskaitos duomenimis, tokiu būdu užtikrinant, jog dokumentų nebūtų galima modifikuoti, o tai ne tik skaidrina procesus, bei apsaugo nuo PVM grobstymo, bet taip pat gali veikti, kaip prevencinė priemonė (žinojimas, jog procesai yra stebimi ir automatizuoti, gali sustabdyti nuo nelegalios veikos pradėjimo). Lenkija naudoja DI/ MM „STIR“ sistemą, kuri kasdien praneša apie sąskaitų ir kliringo duomenis apie visas mokesčių mokėtojų atliktas operacijas, o tai leidžia realiuoju laiku aptikti nelegalios veikos požymius. Tuo tarpu Italijos mokesčių institucijos naudoja "VeRa" DI algoritmą, kuris lygina mokesčių deklaracijas, pajamas, nekilnojamojo turto įrašus, banko sąskaitas ir elektroninius mokėjimus, ieškodamas neatitikimų – nurodoma, jog šios sistemos pagrindu aptikta daugiau kaip 1 mln. aukštos rizikos atveju. Aptikus neatitikimus, mokesčių mokėtojams išsiunčiami laiškai su prašymu patikslinti duomenis, o tai tampa puikia prevencine priemone pradedant nuo švelniosios galios bei leidžiant asmenims pasitaisyti.

Verta pažymėti algoritmų naudojimą ir paprastoms administracinėms ar monotoniškoms užduotims atlikti, pvz.: Rumunija, kuria pokalbių robotą, kuris padėtų geriau orientotis viešųjų pirkimų procesuose. Lietuvoje sukurta „Viesieji Pirkimai AI“ sistema, kuri analizuoja Centrinės viešųjų pirkimų informacinės sistemos duomenis ir identifikuoja aktualius viešuosius pirkimus pagal vartotojo veiklos sritį, pateikia paaiškinimus, konkurso sąlygas, sumažina rankinio darbo kiekį, bei padeda rengti atsakymus į tiekėjų klausimus. Algoritminės technologijos naudojamos ir paprastoms

socialinėms paslaugoms gauti, tam jog paslaugos būtų suteiktos greičiau, atlaisvinti žmogiškieji resursai, tačiau tai turi papildomą naudą, kadangi tokiu būdu yra išvengiama kontakto su žmogumi, o tai sumažina galimą korupcijos riziką. Suomija integravo net 26 programinius robotus, kurie automatizuoja apie 70 skirtingų procesų nuo sąskaitų faktūrų tikrinimo iki registrų atnaujinimo. Šiais būdais ne tik yra sumažinamas žmogiškų klaidų skaičius, padidinamas darbuotojų pasitenkinimas darbu, bet ir stiprinama skaidresnė bei atsparesnė korupcijai aplinka.

Analizės metu, aptiktas Danijos bei Nyderlandų pavyzdys puikiai iliustruoja netinkamai taikomų DI technologijų neigiamus padarinius. Šiose šalyse DI grįsta technologija, skirta socialinių išmokų kontrolei, neproporcingai žymėdavo pažeidžiamas visuomenės grupes (neįgaliuosius, mažas pajamas gaunančius asmenis – kam iš esmės šios išmokos yra aktualiausios). Šios sistemos rinko itin jautrius duomenis apie pilietybę, kilmės šalį, šeimyninius ryšius ir formavo diskriminaciją lemiančius rizikos profilius, dėl kurių asmenims būdavo atimta socialinė parama arba teko mokėti baudas. Viena iš jų „SiRi“ Nyderlandų teisme buvo pripažinta, kaip neteisėta, dėl privatumo bei nediskriminavimo etikos principų pažeidimų. Tai tampa puikiu pavydžiu, kai technologijos yra netinkamai sukurtos bei naudojamos be papildomų apsauginių žingsnių.

Svarbu pastebėti, jog analizuojant ES šalių informaciją apie taikomas DI sistemas – retu atveju buvo nurodomi etikos principai. Būtent Vokietijos „MaLeFiz“ projekte buvo pabrėžiama, kad DI sprendimai turi būti paaiškinami, patikrinami bei veikti skaidriai. Taip pat Bulgarijos „BgGPT“ – pokalbių asistentas, leidžia vartotojams matyti pateikiamų atsakymų šaltinius, tokiu būdu asmenys gali patikrinti informacijos pagrįstumą. O tuo tarpu Slovėnijos projektas „SKRINJA“ (duomenų analizės platforma) orientuotas į GDPR reikalavimų atitikti, nurodo jog diegiant technologijas galima suderinti duomenų apsaugą bei inovacijas.

Iš visų 27 ES šalių, Čekija, Slovakija bei Kipras neturėjo viešai prieinamos informacijos apie naudojamas algoritmines technologijas, kurios prisidėtų prie antikorupcinės aplinkos gerinimo. Tačiau tokios informacijos trūkumas nebūtinai reiškia, kad minimos šalys apskritai nenaudoja jokių technologijų – šį rezultatą galima sieti su viešos komunikacijos stoka bei požiūriu, jog tai neturėtų būti viešai prieinama informacija. Komunikacija viešajame sektoriuje yra itin svarbu, nes visuomenei teikiama informacija, kuria bendrinio skaidrumo jausmą, o žinios apie naudojamas priemones įvairaus, nelegalaus elgesio aptikimui gali veikti, kaip prevencinė priemonė. Teoriniu lygmeniu tai liečia ir racionalaus pasirinkimo teoriją – kuo asmuo labiau jaus, jog jo potencialiai neteisėti veiksmai gali būti efektyviai aptikti, tuo dažniau jis svarstys nevykdyti teisės pažeidimų.

Apibendrinant, daugiausia rastų sistemų, vienaip ar kitaip yra taikomos viešųjų pirkimų procesams stebėti, anomalijoms bei riziką keliantiems veiksniams aptikti. Iš visų ES šalių sistemų –

funkcionalumu bei tikslingumu pasižymėjo Italija, Prancūzija bei Belgija. Šalys taip pat ganėtinai plačiai taiko algoritmines technologijas finansinių srautų stebėjimui bei mokesčių kontrolei vykdyti, kuri gali pasitarnauti norint aptikti nelegalias veikas, kai asmenys aktyviai siekia slėpti turimą turtą. Retu atveju paskelbtos naudojamos sistemos turi etikos principų aprašymus ar kitus saugumo rodiklius, o tyrimo metu rastos žalingos sistemos tik sustiprina šių aspektų poreikį. Verta pabrėžti, jog rastų sistemų kiekis stipriai priklauso nuo šalies komunikacijos lygio, o viešai skelbiamos sistemos gali tapti prevencine priemone stiprinant antikorupcinę aplinką.

2.3. Kokybinis tyrimas: mokslininkų ir specialistų įžvalgos

Šioje tyrimo dalyje buvo analizuojami dviejų grupių interviu: DI srities mokslininkų bei specialistų – dirbančių su antikorupcinės aplinkos gerinimu. Analizės metu siekta atsakyti, kaip mokslinės bendruomenės ir specialistai vertina algoritminių technologijų pritaikymą antikorupciniam darbui. Taip pat aptariami praktiniai šių technologijų naudojimo būdai, taikymo metu iškylantys iššūkiai ir net galimi jų sprendimo būdai. Galiausiai aptariamos šių technologijų galimybės, praktinėje šios temos erdvėje.

Algoritminių technologijų vertinimas, nauda bei pritaikomumas:

Interviu pradžioje dažniausiai nuskambėdavo pasisakymai, jog nei mokslininkai nei specialistai nežino specifiskai antikorupcinei veiklai skirtų algoritminių įrankių Lietuvoje (nei užsienyje) „Lietuvoje tai arba atrodo, kad nieko nevyksta su tais klausimais, arba jeigu vyksta, tai tikrai apie tai nekalba garsiai.“ (S4), tačiau plėtojant pokalbį su specialistais atsirasdavo praktinių sričių, kuriose jau pasitelkiamos algoritminės technologijos, o mokslininkai atsimindavo arba sugalvodavo DI taikymo sritis, kurios visgi prisideda prie antikorupcinės aplinkos stiprinimo. Pašnekovai dalinosi įvairiais pavyzdžiais iš Lietuvos viešojo sektoriaus patirties, kurie padeda suprasti šių technologijų taikymo galimybes.

Interviu dalyviai dažnai pabrėžė, kad tinkamai pritaikyti algoritminiai įrankiai gali padidinti darbo efektyvumą ir pašalinti žmoniškojo faktoriaus daromą žalą, mokslo atstovė pabrėžė, jog „<...> DI nedomina kyšiai <...>“ (M1). Šią mintį palietė ir specialistė, jog korupcijos rizikos gali kilti dėl subjektyvaus žmogaus įsikišimo į procesus, o procedūrų automatizavimas gali užkirsti tam kelią „<...> CPO.lt elektroninis katalogas yra pagrindinė priemonė Lietuvoje vykdyti skaidrius pirkimus, skaidrius viešuosius pirkimus, nes tai yra procesas, kuriame žmoniškasis faktorius, kuris ir yra iš esmės pagrindinis korupcijos priežasties reiškinys yra eliminuojamas. <...>[procesai] vyksta automatinio būdu, be žmogaus įsikišimo“ (S1). Automatizuota sistema padeda užtikrinti skaidrumą,

nes sumažėja galimybių nesąžiningai paveikti procesų rezultatus. Kitas dažnai įvardintas privalumas, tai jog DI gali apdoroti didelius duomenų kiekius greičiau, nei pajėgtų žmogus, aptikti dėsningumus, paspartinti duomenų analizę ar „raudonų vėliavų“ aptikimą „*Technologijos tikrai gali padėti apdoroti duomenis ir galbūt nustatyti, kokios indikacijos, <...> parodo, jog yra rizika kažkokios korupcinės veiklos*“ (M7). Šie duomenys rodo, jog DI gali padidinti institucijų veiklos našumą, atlaisvindamas specialistus nuo monotoniškų procesų, padėdamas atlikti kūrybinį darbą. Verta pabrėžti, jog lyginant su specialistais, mokslininkai, išvardindavo daugiau pozityvių bei naudingų DI galimybių, nurodo, kad tai didina darbo spartą ir tikslumą, mažina žmogiškojo faktoriaus klaidas stiprina stebėseną ar net prevenciją, o specialistai dažniau įvardindavo darbo greičio pokyčius, kurie bendrai gali pozityviai įtakoti antikorupcinės aplinkos gerinimo procesus.

Specialistai interviu metu nurodė, jog viešajame sektoriuje DI „*<...> daugiau naudojama procesų našumui, optimizavimui, kažkokių rutininių procesų palengvinimui.*“ (S4). Ši grupė nemažai dalinosi pozityvia patirtimi, kaip naudojasi generatyviniu DI įrankiu (pvz.: „ChatGPT“, „Microsoft CoPilot“). Akcentuota, kad tokios priemonės ženkliai sutaupo laiko rengiant dokumentus, apibendrinant informaciją ar atsakant į įvairius klausimus „*<...> ką anksčiau reikėdavo googlint, tą dabar gauni paprasčiau, vieno prompto [užklausa] principu. Tai jeigu tai palengvina ir sutaupo laiko, tai kodėl to nedaryti?*“ (S3). Taip pat pabrėžiamas ir naudojimo platumas „*<...> [naudoja] absoliučiai visiems darbo procesams. Tai jisai [„ChatGPT“] pagrindinis įrankis ir yra naudojamas mano veikloje tiek, kiek ji yra susijusi ir su antikorupcinės aplinkos stiprinimo funkcijomis, tiek ir su mano tiesioginėmis funkcijomis. <...> gali parašyti nebe per dieną, o per penkiolika minučių. <...> turi potencialo savo efektyvumą labai stipriai didinti, jeigu tu to nori*“ (S1). Pateiktas sėkmingas pavyzdys, kaip pasitelkiant generatyvų DI, ne tik lengvinama biurokratinė našta, tačiau ir ieškoma dėsningumų tarp laiminčių organizacijų viešuosiuose pirkimuose. „ChatGPT“ su vizualizacijų įskiepais gali sukurti grafinius ryšių žemėlapius tarp perkančiųjų organizacijų ir tiekėjų, leidžiančių matyti paslėptus ryšius ar galimus susitarimus „*tiesiog 3D schemeje <...>, bet viskas žiauriai easy [lengva], grafikų paišymas iš turimų duomenų. Vienas geriau pasitvirtinusių tokių metodų yra, nes mes jau kelintą kartą jį naudojame, su viešais pirkimais <...>*“ (S3). Tai rodo, kad net viešai prieinami, generatyvūs DI įrankiai, kūrybiškai pritaikyti, gali tapti galingu ginklu korupcijos rizikų analizei.

Verta paminėti, jog specialistų minimas generatyviojo DI naudojimas gali kelti rizikų, nors interviu metu buvo įsitikinta, kad specialistai naudojami tik vidiniu „ChatGPT“ paketu (t.y. sukurtas vidinis, mokamas kanalas, kurio duomenys nėra naudojami sistemos apmokymui), kitos paminėtos generatyvaus DI sistemos kelia susirūpinimą. Interviu metu buvo minimos „CoPilot“ bei „Deepseek“ sistemos, kurios veikia panašiu principu kaip ir „ChatGPT“, tačiau „Microsoft“ įskiepis neturi savyje funkcijų vidiniam naudojimui, todėl į sistemą keliami duomenys nėra apsaugoti. Nors ir minimas

specialistų abejingumas naudoti „Deepseek“ – suvokimas apie jos grėsmės paviršutinis. „Deepseek“ sistema, sukurta Kinijos subjektų, kelia skaidrumo, duomenų privatumo, saugumo rizikas, o daugelis ES šalių ragina nesinaudoti šia sistema ar net uždraudžia naudotis ja viešajame ir privačiajame sektoriuose.

Kaip minėta, CPO elektroninis katalogas jau dabar automatizuoja didelę dalį pirkimo procedūrų „<...> *pateikia pasiūlymą vokai atsiplėšia automatiškai, eilė generuojami automatiškai, sutartis sudaroma automatiškai* <...>“ (S1), nors pašnekovė nenurodė šios sistemos algoritmų specifikos iš pateiktos medžiagos teorinėje dalyje bei atsižvelgiant į ES šalių gerąsias praktikas galima daryti išvadą jog sistema gali būti paremta blokų grandinės technologijos principu. Taip pat be esamų sprendimų, kuriamos ir naujos DI priemonės, interviu metu buvo pasidalinta ir apie CPO vystomą projektą, kuris „*Dirbtinio intelekto pagrindu veikiantis instrumentas būtent kainų palyginimui, suradimui palyginimui, sutaupymo skaičiavimui ir analizei.*“ (S1). Toks įrankis pasak specialistės leistų automatiškai aptikti nepagrįstai aukštas kainas bei sutaupyti biudžeto lėšas, ne tiesiogiai, tai būtų svarbi antikorupcinė funkcija, nes identifikuotų galimą piktnaudžiavimą kainodara. Kita tarnyba neseniai iniciavo vidinį DI projektą – „*robotuką*“ (S5), kuris būtų apmokytas jų kaupiamais duomenimis, galėtų greitai atsakyti į darbuotojų užduodamus klausimus (nuorodos į vidinius dokumentus, ataskaitas ar kitus šaltinius) – tokioms iniciatyvoms pritarė ir mokslininkų grupė. Pašnekovai taip pat minėjo nesėkmingą, bet dar bandomą vystyti DI projektą viešųjų pirkimų priežiūrai „SauleIS“ „<...> *kaip suprantu, nepavyko*“ (S4), „<...> *tiesiog nepavyko jos sukurti.*“ (S5). Ši sistema buvo skirta analizuoti viešųjų pirkimų duomenis, identifikuoti rizikas, jas vertinti. Nurodoma jog projektas nepavyko dėl tiekėjo kaltės, svarstyta, jei „<...> *tarnybai duotų neribotus kaštus, turbūt pabaigtų [projektą] „Saule“.* <...> *tikimės, kad bus kažkada.*“ (S5). Tai leidžia manyti, jog finansų ir pajėgumų trūkumas, o ne DI pritaikomumo stoka, tampa pagrindine kliūtimi.

Kadangi korupcinis veikimas gali atsispindėti ir finansiniuose srautuose, interviu dalyviai plačiau aptarė algoritminių priemonių pritaikymą finansų sektoriuje. Dalis tiriamųjų akcentavo pinigų plovimo prevencijoje taikomus įrankius (M5, M6, S4). Mokslininkai pateikė „kažkur girdėtą“ informaciją, pvz. jog VMI stebi medijas ir jose vykstančią galimai nelegalią komercinę veiklą (M5). Finansų srityje, patys specialistai nurodė, jog naudojamos algoritminės sekos „<...> *[tikrina] kiekvieno Lietuvos gyventojo pajamų išlaidų balansą. <...>[nustatyti] ar jo išlaidos viršija pajamas*“ (M2), šie įrankiai turi analizuoti didelį duomenų kiekį (įvairių registrų duomenys, deklaracijos, bankinės apyvartos, likučiai ir kt.). Tačiau verta pabrėžti, jog būtent specialistai finansų srityje buvo labiausiai akcentuojantys didžiulius DI taikymo sunkumus bei apribojimus. Interviu metu buvo itin aiškiai iškomunikuota, jog tiesiogiai gyventojus liečiančiose srityse, vengia daryti prielaidas remiantis DI „<...> *mes netaikome jokio dirbtinį intelekto, skaičiuojant gyventojų pajamas išlaidas,*

<...> negalime šitoj vietoj daryti prielaidų, o mes turim eiti labai konkrečiai nes tie klausimai gyventojui labai jautrūs <...>, gali atsirasti bereikalingos įtampos“ (M2). Toks požiūris gali turėti ne vieną reikšmę: specialistai supranta visuomenės baimes dėl DI, mano jog visiškas automatizavimas gali kelti nepasitikėjimą darbo rezultatais, trūksta žinių apie šių technologijų teikiamą naudą ar rizikų valdymą. Tiesa, tie patys specialistai nurodo, jog šiuo metu naudojami algoritmai padeda mažinti neatitiktį turto ir pajamų deklaravime, greičiau atlikti reikiamus darbus.

Interviu metu mokslininkų grupė minėjo DI pritaikomumą teismuose – pažymima nauda atliekant bylų nuasmeninimą, ieškant teismų praktikos, atliekant administracinį darbą (M1, M2, M4, M6), išskirta mintis, jog DI gali efektyvinti teismų darbą *„Kokia yra prasmė nuteisti žmogų dėl korupcinio nusikaltimo po 10 metų, kai jis po 10 metų vis dar bus? Arba pasakyti, kad jis nekaltas po 10 metų, tai tas greitis irgi turi labai didelių plusų. <...> neabejoju, kad teisėsaugoje dirbtinis intelektas plis toliau <...>“*, (M2), žinoma tuo pačiu tenka susidurti su iššūkiais, jog net ir taikant DI teismuose galime nepasiekti gerų sistemų veikimo rezultatų dėl gana mažo kiekio korupcinio pobūdžio bylų (sistemų apmokymui reikiami duomenys), o prasti rezultatai gali lemti teisėjų šališkumą. Minimas ir didelio masto „Čekiukų“ skandalas, pastebėta jog prokurorai vis dar nepritaikė DI bei viską atlieka rankiniu būdu (M5), o tai nurodo, kaip teisingai pritaikytos technologijos išties palengvintų bei pagreitintų teisėsaugos darbą sprendžiant korupcinio pobūdžio bylas, ko pasakoje sprendimo priėmimo greitis galėtų pozityviai įtakoti skaidrumą.

Apibendrinant, nors abi grupės pritaria dėl DI naudos, visgi mokslininkai pabrėžia teorinę naudą bei potencialą bei gilesnių praktinių panaudojimo variantų, o specialistai labiau orientuojasi į siauresnį šių technologijų pritaikomumą, pažymėdami praktikoje veikiančius metodus. Taip pat pastebima, jog aktyviai DI taikančios institucijos yra daug pažangesnės bei pozityvesnės inovacijoms, tačiau iškelia klausimą ar specialistai naudojantys generatyvųjį DI yra supažindinti su jo rizikomis. Priešingai – ne tokios inovatyvios įstaigos, nors ir norėtų šiomis technologijomis palengvinti darbo procesus, pažymi nepasitikėjimą algoritminėmis technologijomis bei išreiškia baimę, nežinomybę dėl jų taikymo ateityje. Šioje dalyje pateiktas ne vienas pavyzdys, kaip šio tipo technologijos yra taikomos Lietuvoje, norint gerinti antikorupcinę aplinką bei spartinti institucijų darbo procesus. Šiuo pagrindu galima tvirtai teigti, jog DI technologijos ne tik jau dabar naudojamos viešajame sektoriuje, bet ir kuriami įvairaus tipo projektai padėsiantys įdarbinti DI įrankius gilesnioms korupcijos analizėms atlikti.

Iššūkiai ir kliūtys diegiant bei naudojant algoritminius įrankius:

Surinktoje interviu medžiagoje išryškėjo nemažai praktinių, organizacinių ir teisinių iššūkių, stabdančių plačiau diegti algoritmines technologijas antikorupcinei aplinkai stiprinti. Šie iššūkiai

apima specialistų ir žinių stoką, finansinius ir technologinius ribojimus, duomenų prieigos bei kokybės problemas, taip pat institucinės kultūros ir valdymo aspektus.

Beveik vieninga specialistų nuomonė buvo, jog trūksta žmonių, gebančių kurti ir pritaikyti DI sprendimus viešajame sektoriuje. Specialistai nurodo jog „<...> buvo labai liūdna. Realiai todėl, kad rasti dirbtinio intelekto ekspertus, kurie ne tik mokytų rašyti promptus [užklausa] arba paaiškintų, kad dabar yra tūkstančiai įrankių, dirbtinio intelekto ir jais jau reikia naudotis. <...> mums nepavyko beveik rasti <...>“ (S1). Specialistė pažymėjo ir kitą atsiradusią bėdą, jog net ir surengus mokymus pastebi, kad jų specialistams „nedega akys“ (S1). Pažymima, jog „<...> atrodo ne visi gal žmonės tą naudą įžvelgia, gal kartais atrodo, kad kam čia to reikia?“ (S5), tai gali būti dėl didelio žinių atotrūkio, kuri pažymi kita specialistė – viešojo sektoriaus darbuotojams dažnai trūksta suvokimo kas yra DI, kaip jis veikia, todėl jiems sudėtinga juo pasitikėti ir naudoti (S4). Prie pačio algoritminių technologijų diegimo apsunkinimo prisideda ne tik žinių trūkumas, tačiau ir daug organizacinio neaiškumo „mes dar nesam pasiruošę mums reikia labai aiškiai susireguliuoti, [kur, ką ir kiek galima taikyti]<...> nu tiesiog dėl saugumo.“ (S2). Akcentuojama, jog svarbi vadovybės lyderystė „<...> gaunasi galbūt net nebe technologinis, o valdysenos elementas. <...> [iniciatyvus specialistas] neša tas naujoves, kurias vadovas nuleidžia į apačią“ (S1). Šie rezultatai rodo, kad darbuotojai gali ir toliau vertinti DI kaip nebūtiną įrankį, kai organizacijoje nėra aiškos žinutės, vizijos, organizacinių sprendimų ir palaikymo vystyti inovacijas.

Specialistų trūkumas yra ne tik dėl to, jog sunku atrasti asmenis, kurie turėtų tarpdisciplininių žinių (M4, M7, M3) (sistemų diegimui reikia ne tik žinių apie DI, tačiau ir pačios srities žinių, kur sistema bus taikoma), bet taip pat siejamas su finansinių resursų stoka „<...> [specialistų] norėtume turėti daugiau, bet čia susidūrėme su finansų problema, na tiesiog jie yra sunkiai įperkami, <...>“ (S2). Net ir palyginamai pažangesnės institucijos (apklaustųjų rėmuose) susiduria su finansinių resursų stoka „mums pasirodė per brangu“ (S1), „Faktas, kad numeris vienas tai finansinės, nes po finansinėm eina žmogiškieji ištekliai, nu technologijų ištekliai,“ (S3), tuomet specialistai atsimuša į kliūtį, jog ne viską gali padaryti patys, todėl perka paslaugas iš vykdytojų. Anksčiau minėtas projektas „SauleIS“, pasak apklaustųjų neįvyko dėl tiekėjų kaltės, tai nurodo papildomą iššūkį, kai projektai nėra įgyvendinami dėl išorinių priežasčių. Taip pat sudarant sutartis tiekėjai turi praeiti atrankos procedūras, patikrinimus, kadangi sistemų diegimo metu prisiliečiama prie itin jautrių duomenų (S2), o tai apsunkina inovacinį procesą. Tai rodo, kad lėšos, biudžetinėse įstaigose apriboja algoritminių technologijų diegimą, tačiau net ir turint finansinių resursų atsimušama į kompetencijų ir tiekėjų niuansus. Šios problemos sukuria „užburto ratą“ – be finansų sunku pasamdyti specialistus ar mokyti savus sistemų kūrimo ir jų taikymo, o be specialistų ir sistemų kūrimo sunku parodyti rezultatą, kuris galėtų pagrįsti didesnę finansavimą.

Beveik visi pašnekovai vienaip ar kitaip palietė duomenų klausimą, tačiau išsiskyrė grupių nurodomos problemos: mokslininkai labiau akcentavo duomenų prieinamumą, jų kokybę, o specialistai nors ir minėdavo duomenų kokybės trūkumus, labiau plėtojosi ties BDAR bei kitais saugumo elementais, kurie riboja naudojimąsi duomenimis algoritminėse technologijose. Po BDAR „<...> pasidarė truputėlį sunkiau juos gauti iš viešojo sektoriaus institucijų, nes neretai yra gaunamas atsakymas, kad dėl privatumo negali suteikti duomenų“ (S4), kiti specialistai nurodo „*Tai pats pagrindas yra BDAR. <...> dirbtinio intelekto naudoti mes negalime <...>. Mes galbūt galim paklausti kokius metodus naudoti analizei ar kažką tai bet tiesiogiai ne [specialistai tikėtina mintyje turi tik „ChatGPT“]*“ (S2). Su ta mintimi nurodomas ir problemos sprendimo būdas ateityje „*kai jie bus vidiniai <...> jau galėsi dirbt su savo duomenimis, kurie nėra vieši ir iš jų gauti naujus rezultatus, analitinius rezultatus, kurių gal tu nematei arba net neturėjai minties, kad gali tuos rezultatus ten matyti ar juos atrasti*“ (S3), bet kaip ir minima anksčiau, dauguma aspektų atsimuša į finansinius resursus.

Tuo tarpu mokslininkų grupė beveik vienareikšmiškai nurodo duomenų gilesnius trūkumus „*Lietuvoje yra problema, kad į duomenis <...> žiūrėjo kaip į verslą <...> visi čia perka net teisėsaugos institucijose, moka už gaunamus duomenis.*“ (M5), taip pat jie yra neprieinami nevyriausybinėms organizacijoms (prieiga galėtų prisidėti prie skaidrumo stiprinimo). Dažnai duomenų atvėrimas ar prieigos siejamos su teisiniais iššūkiais, tokiais kaip jau minėtas BDAR bei naujai išleistas DI aktas – sudėtinga šukuoti (ang. „Scraping“) internetą algoritmų apmokymui. Pažymima, jog net ir turint įvairių registrų duomenis, pvz.: privačių interesų, galutinių naudos gavėjų, lobistų, turto deklaracijos – yra pildomos pačių asmenų, todėl šie duomenys gali būti netikslūs, klaidinantys „*savideklaracijomis nelabai galime pasitikėti*“ (M5).

Taip pat ties privatumo klausimu iškyla etikos dilema, ją akcentuoja mokslininkų grupė (M2, M5, M4). Klausimas išlieka, kur yra proporcingumas tarp skaidrumo ir asmens duomenų privatumo „*<...> politiko žmona ar šeimos nariai. Jeigu juos visus sudėti į AI? Žodžiu, mums kaip čia tokia tema, kur asmens duomenų apsauga ir jos svarbis tai svarbu*“ (M5). Pasitelkiant DI sistemas galima vienu metu įrašinėti, transkribuoti, sekti lokacijas, „*o kur tai būtų nelegalu jau? <...> asmens duomenų apsauga irgi yra labai svarbu ir tiek bendrai teisėsaugoje, tiek ir norinti korupcinius tuos ryšius nustatyti*“ (M4). Mokslininkai taip pat minėjo ir įvykusius diskriminacijos rezultatus užsienyje (Nyderlandų atvejis) (M1, M4, M5, M6, M7), kai kurie akcentavo ir galimą pasinaudojimą šiomis technologijomis, kai jos taikomos nelegaliai veiklai atlikti, rengti mitingus. Tokie atvejai nurodo sisteminės klaidos galimybes ir didelę svarbą tinkamam sistemų kūrimui, apmokymui duomenimis ir nuolatinę priežiūrą. Beveik vienareikšmiškai sutinkama, jog tokios sistemos gali būti tik pagalbiniai įrankiai, o galutinis sprendimas turi būti priimtas žmogaus. Mokslininkai taip pat palietė DI sistemų

veikimo principą, tampa sunku užtikrinti skaidrumą, bei paaiškinamumą, kai sistemos veikia, kaip „Juodosios dėžės“. Tik maža dalis specialistų paminėjo nesaugias sistemas, kaip „Deepseek“(S1) arba korumpuoto DI galimybę (S4). DI etikos principai taip pat buvo paminėti tik paviršutiniškai (minimas skaidrumas, nešališkumas). Tarp dviejų tiriamųjų grupių, šiame žinių lauke, matoma nemaža atskirtis, specialistai šių sistemų neveiksumą arba grėsmę dažnai mato paviršutiniškai, o mokslininkai akcentuoja daugiau giluminių DI galimų grėsmių.

Vis dėlto mokslininkai nurodo įvairius sprendimo būdus DI iššūkiams spręsti, svarbu pagerinti duomenų prieigą (atverti duomenis)(M2), sprendžiant privatumo problemą – automatiškai pašalinant jautrias detales (naudojant DI)(M3), nes tai didins skaidrumą bei stiprins antikorpacinę aplinką. Sutvarkyti įvairių registrų duomenys (M5, S4) gali tapti itin stipriu įrankiu įgalinant algoritmines technologijas, tačiau kad tai įvyktų reikia aiškaus politinio lygmens apsisprendimo atlaisvinti, kai kuriuos ribojimus stabdančius inovacijų plėtrą (S2, S4). Specialistai daugiau akcentuoja ekspertinių mokymų teikiamą naudą, kurios pagalba darbuotojai gali labiau suprasti šių technologijų pritaikomumą kasdienėms veikloms atlikti, lygiagrečiai pabrėžiamas tarpinstitucinis komunikacijos vaidmuo bei dalinimasis gerosiomis praktikomis ne tik Lietuvoje bet ir su užsienio valstybėmis. Švietimo būtinumui pritaria ir mokslininkai *„Tam, kad asmenys, kurie ateina dirbti į viešąjį sektorių, turėtų supratimą ir gebėjimą patikrinti technologijas, žinotų, kur ieškoti informacijos, kaip ją atsirinkti, turėtų tam tikras kompetencijas <...>“* (M7). Dauguma tiriamųjų nurodė poreikį „prisijaukinti“ technologijas įvairiais būdais (didinant švietimą, mažinant inovacinį atotrūkį). Specialistai taip pat nurodo vidinių sistemų svarbą, o mokslininkai daugiau orientuoti į duomenų atvirumą bei jų kokybės gerinimą.

Apibendrinant, mokslininkų ir specialistų žinios ir patirtys su DI iššūkiais skiriasi, tačiau yra ir dėsningumų. Mokslininkai pabrėžia sisteminius iššūkius, susijusius su duomenų prieiga, jų kokybe, kurie apsunkina algoritminių technologijų diegimą, o specialistai akcentuoja duomenų iššūkius ne iš kokybės ar prieinamumo pusės bet iš jų saugumo bei reguliavimo – BDAR perspektyvos, nurodant jog tai apriboja inovacijų naudojimą bei kelia daug neaiškumo. Mokslininkai interviu metu buvo orientuoti į kylančius etikos klausimus susijusius su privatumo ir skaidrumo derinimu. Tuo tarpu specialistai buvo daugiau orientuoti į praktinius aspektus – kompetencijų, finansų bei specialistų stoką. Nepaisant tam tikro grupių įžvalgų atotrūkio – abi sutaria, dėl būtinybės stiprinti specialistų švietimą, ugdyti kompetencijas bei kurti aiškią politiką dėl duomenų ir algoritminių technologijų naudojimo viešajame sektoriuje.

DI Etika ir algoritminių technologijų reguliavimas:

Neišvengiamai, šioje srityje, susiduriama su DI etikos principais bei šioms sistemoms taikomo reguliavimo niuansais. Apklausiant abi grupes, viso tyrimo rėmuose, pastebėta ryškiausia atskirtis – specialistai arba nėra susipažinę su DI reguliavimu ir jam taikomomis etikos taisyklėmis, arba apie tai kalba itin paviršutiniškai, atsižvelgdami tik į technologijų naudą savo darbui.

Visi mokslininkai vienaip ar kitaip išsireiškė, jog etikos principai, gairės negali efektyviai apsaugoti nuo DI keliamų rizikų, „*[laikytis gairių] tai nėra privaloma*“ (M2), „*jos yra tokios rekomendacinio pobūdžio*“ (M3), „*mano nuomone su rizika jie nieko nepadedą*“ (M6). Tačiau kai kurie nurodo jų kitokią prasmę „*DI aktas neatsirado iš niekur <...> sunkumai, susiję su etikos standartais, yra tai, kad juos ne taip lengva paversti praktiniais veiksmais, todėl jie dažniausiai tarnauja kaip tam tikra koncepcija*“ (M2). Anksčiau aptarti etikos principai atspindi naujai suformuotame reglamentavime, jie naudingi apmokant specialistus, kurie kuria sistemas (M2). Įvairių gairių bei principų veiksmingumas, mokslininkų grupės nuomone, priklauso nuo to, kaip jie bus pritaikomi praktiškai – ir šioje potemėje grįžtame prie organizacinės kultūros. Iš rezultatų galime formuoti mintį, jog techninė rizikų kontrolė turi eiti koja kojon su pačių naudotojų etine refleksija. Kalbant apie DI akto turinį dažnu atveju, mokslininkai nurodo jog „*<...> bet koks reglamentavimas ir dabartinis reglamentavimas yra geriau negu nieko <...>*“ (M4), tačiau patys mokslininkai neretu atveju susiduria su reglamento trūkumais, kadangi pats aktas yra sukurtas rizikos lygių principu – yra daug neaiškumo bei trūksta detalesnių akto išaiškinimų. Pateikiama „*daug kritikos šiam aktui dėl to, kad sakoma, kad galbūt stabdys inovacijas ir ribos galimybes toliau diegti technologijas*“ (M2), taip pat keliami klausimai: „*<...> nežinau kam to reikia stabdyti inovacijas?*“ (M6), „*Kiek įmanoma teisiškai sukontroliuoti?*“ (M5). Ši grupė kėlė klausimus ar tikrai savarankiškai daromi įvertinimai (technologijų rizikai nustatyti) yra korektiška prieiga rizikų kontrolei, ar tinkamai bus vertinami įrankiai, kurie gali būti naudojami tiek administracinėms užduotims atlikti, tiek aukštos rizikos veiklai (pvz.: „ChatGPT“ gali būti naudojamas ne tik atsakinėjant į laiškus ar informacijos paieškai, bet ir jautrių duomenų analizei atlikti, o pagal DI aktą abu šie procesai turi visai skirtingus rizikos lygius), bei tai jog vis dar nėra itin aišku, kas turi atsakyti už galimas žalas. Visa tai nurodo, jog mokslinė bendruomenė įžvelgia naujo reguliavimo naudą, tačiau, kaip ir buvo minėta interviu metu – naujam aktui prireiks laiko, kaip ir BDAR, kol jis taps pritaikomas bei aiškus praktikoje – o kol kas pravartu žinoti, bent ko negalima daryti (pagal DI aktą).

Tuo tarpu specialistai neturėjo pakankamai žinių apie DI akto, etikos bei gairių turinį, dažnu atveju į šia tema užduodamus klausimus atsakydavo tik iš profesinės pusės „*sau taikau principą, kad nu tu esi atsakingas, ypač darbinėj aplinkoj, ką tu su jom [technologijomis] darai, nepaisant kokie ten aktai parašyti ar neparašyti. <...> teisiniu reguliavimu, tai kažkaip neteko dar susidurti, nežinau ar teks. <...> Tai dėl to ar čia labai reikėtų pradėti riboti ar stabdyti procesą, aš prieš*“ (S3).

Specialistai nurodydavo, jog reikia laikytis tam tikrų standartų dėl kibernetinio saugumo, etiškas naudojimas jiems svarbus dėl duomenų apsaugos, tačiau visgi pastebėta, kad specialistai yra daugiau orientuoti į gerų rezultatų siekį, su užuomina, jog visi DI technologijų ribojimai gali varžyti „<...> mūsų veiklai pritaikyti būtų sudėtinga nes ten yra labai daug sąsajų arba reikalų su BDAR“ (S2), „<...> kurie naudoja, apie tai nedaug galvoja. Na, jie ima ir vartoja, ką jie prieina, ką jie gauna, jeigu vartoja.“ (S1). Minima jog etišką DI naudojimąsi ir kūrimą, galima užtikrinti švietimu „<...> mes galėsime užtikrinti jų toki saugesnį panaudojimą ir to reguliavimo nereikės tokio griežto.“ (S4). Tai kelia susirūpinimą, kai viešojo sektoriaus įstaigų darbuotojai nėra tinkamai supažindinti su taikomu reguliavimu arba pagrindinėmis DI etikos gairėmis, kurios gali suteikti teisingo bei efektyvaus darbo rezultatų. Kyla klausimas, kiek iš tikro šios technologijos yra etiškai taikomos (galbūt atsakymai įtakoti socialinio pageidaujimumo efekto) institucijų viduje ir kiek esamo reguliavimo neaiškumas daro įtakos šių technologijų implementavimo baimei?

Apibendrinant, šioje tyrimo dalyje atsiskleidė bene didžiausias žinių bei požiūrių atotrūkis tarp mokslininkų bei specialistų. Mokslininkai skeptiškai vertino DI etikos gairių veiksmingumą, nurodydami jog tai rekomendacinio pobūdžio įrankis ir realiai neapsaugo nuo DI rizikų. Taip pat pažymimas DI akto reikalingumas, tačiau kartu nurodoma jog jo taikymas praktikoje kelia daug neaiškumų. Specialistai neturėjo pakankamai žinių apie DI reguliavimą, orientacija kryo ties praktine nauda ir rezultatų siekimu, o etikos principus labiau supranta per kibernetinio saugumo ir duomenų apsaugos prizmę. Specialistai taip pat pažymi jog etiškas algoritminių technologijų naudojimas labiau priklauso nuo specialisto požiūrio ir žinių, atsakomybė išlieka naudotojui, todėl iškyla švietimo svarba.

Algoritminių technologijų galimybės antikorupcinėje veikloje:

Interviu metu, tiek mokslininkai, tiek specialistai pasisakė, jog algoritminių technologijų vaidmuo antikorupcinėje veikloje tik augs. Informantai įvardino keletą kryptų, kur šios technologijos būtų naudingiausios jų darbe ar apamai tokioje veikloje. Viena iš itin aktualių sričių – viešieji pirkimai, nurodoma, jog „visuose etapuose viešojo pirkimo dirbtinis intelektas privalo būti naudojamas. Tai ten rinkos analizė. Tikrai taip. Techninių specifikacijų rengimas tikrai taip. Vertinimo kriterijų nustatymas. Tikrai taip. Dokumentų standartizavimas ar patikra, ar ten nežinau lyginimas, ar kažkas dar lyginimas. Tikrai taip. Pasiūlymų vertinimas Tikrai taip.“ (S1). Vykdomi ar bandomi vykdyti projektai susiję su viešųjų pirkimų automatizavimu, nurodo aiškų specialistų norą pritaikyti tinkamas technologijas skaidrumui didinti ir nors trūkta tam tikrų resursų – šiame procese vis tiek įžvelgia didelį potencialą. Įvardinama, jog dėl įvairių deklaracijų savikontrolės susiduriama su abejotina duomenų kokybe (M5, S4), tačiau juos tvarkant ir įdarbinant registrų informaciją, DI technologijoms apmokyti, galime pasiekti aukštų rezultatų. Absoliuti dauguma nurodo dideles

galimybes mažinant administracinę naštą, eliminuojant nekompetencijos klausimus, turint vidinius įrankius, spartinti bei tobulinti duomenų analizės galimybes. Išskirtas potencialas pritaikant algoritmines technologijas pranešimų, skundų nagrinėjimui ar stiprinant pranešėjų apsaugos procesą (M5, S2, S3). Mokslininkai siūlo didesnio stebėjimo galimybes, siejant DI su aero nuotraukomis, finansinių srautų stebėsenai, sumaniųjų kontraktų įdarbinimą (M5, M6), susitikimų analizei: „*su kuo bendrauta, kaip, kokiais klausimais buvo balsuota, kur galbūt prieš tai kokiose asociacijose dalyvauta*“ (M7), socialinių tinklų, naujienlaiškių ar rinkos sentimentų stebėjimui (M6). Pabrėžiama komunikacijos svarba, nes tai veiktų, kaip tam tikra prevencija bei spartintų gerųjų praktikų dalinimąsi tarp institucijų (M5, M3).

Taigi, lyginant dvi interviu grupes pastebėta, jog mokslininkai turi daugiau teorinių žinių ar išradingumo, nurodant, kokius duomenis galima įdarbinti antikorupcinėje veikloje. Specialistai yra daugiau orientuoti į šių sistemų pritaikymą toms užduotims, kurios sukuria biurokratiją, mažesnė dalis jų minėjo galimybes stiprinti analitinę ar prognostinę savo darbo sritį. Tačiau abi grupės pabrėžia algoritminių technologijų potencialą antikorupcinėje veikloje bei nurodo jog šių technologijų naudojimas ateityje spartės.

2.4. Diskusija

Mokslinės literatūros, ES šalių praktikos bei atliktų interviu duomenų analizė atskleidžia ryškią tendenciją – algoritminės technologijos turi didelį susidomėjimą jų pritaikomumu stiprinant antikorupcinę aplinką, tačiau jų įgyvendinimas susiduria su reikšmingais praktiniais iššūkiais. Teorinėje dalyje aptartos šių technologijų naudos: gebėjimas apdoroti didelius duomenų kiekius, pastebėti dėsningumus, identifikuoti „raudonas vėliavas“ – sutampa su empiriniame tyrime gautais duomenimis. Literatūroje pabrėžiama, kad DI priemonės viešajame sektoriuje gali ženkliai didinti analitinį pajėgumą ir užkirsti kelią žmogiškojo faktoriaus nulemtoms klaidoms (pvz.: šališkumui, kyšininkavimui). Praktikoje tą patvirtina ES šalių taikomi sprendimai: beveik visos valstybės diegia algoritmines sistemas viešuosiuose pirkimuose, siekiant automatizuotai aptikti riziką keliančius pasiūlymus, tiekėjų susitarimus, interesų konfliktus. Interviu dalyviai, taip pat buvo daugiau orientuoti į viešuosius pirkimus, bei akcentavo jog tokios technologijos pradedamos kurti ir Lietuvoje. Iš viso darbo duomenų galime daryti išvadą jog viešieji pirkimai yra suvokiami, kaip viena rizikingiausių sričių, kur algoritminiai įrankiai gali turėti didžiausią antikorupcinį efektą bei yra prioritentinė DI naudojimo kryptis – tiek literatūroje, tiek ES šalių praktikoje, tiek ekspertų įžvalgomis. Kita reikšminga sutaptis – finansų sektoriaus stebėseną, kur algoritminės sistemos padeda atskleisti galimas korupcinės veikos apraiškas. ES šalių analizė bei interviu duomenys nurodo, kad DI gali padėti identifikuoti pajamų ir išlaidų neatitikimus, slepiamą turtą, PVM grobstymą. Daugelis ES šalių

taiko analitinius įrankius mokesčių vengimo, fiktyvių sandorių ar neteisėto praturtėjimo nustatymui, o specialistai Lietuvoje patvirtina, kad finansų sektoriuje algoritminiai įrankiai naudojami pajamų – išlaidų balansui tikrinti ir pinigų plovimo prevencijai. Tačiau verta išskirti, jog specialistai finansų srityje susiduria su dideliais duomenų apsaugos iššūkiais bei neaiškiomis DI pritaikomumo/pasitikėjimo galimybėmis.

Svarbu pabrėžti, kad dažniausiai, šiuo metu, praktiškai taikomi algoritminiai įrankiai Lietuvoje, yra skirti biurokratinėms užduotims lengvinti bei spartinti, o retesniu atveju naudojami gilioms analizėms atlikti (didesnė dalis aukštos rizikos sistemų yra tik kūrimo procese). Duomenų analizės metu išryškėjo atskirtis tarp interviu grupių, specialistai daugiau fokusuojasi į konkrečius naudą teikiančius sprendimus (administracinės naštos, tekstų rašymas, klausimynų pildymas, informacijos paieška), o mokslininkai linkę matyti platesnes galimybes (socialinių tinklų stebėjimas, išmaniųjų sutarčių diegimas, įvairių registrų duomenų naudojimas). ES šalių apžvalga taip pat patvirtina nevienodą progresą, kai kurios valstybės išsiskiria novatoriškais projektais, o kitos (įskaitant Lietuvą) viešųjų šaltinių duomenimis kol kas įgyvendina tik pavienės arba mažesnio funkcionalumo sistemas. Tai rodo, jog Lietuvoje, specialistai dirbantys su antikorupcine veikla dar nepakankamai informuoti apie šių technologijų panaudojimo galimybes, o tai patvirtina ir interviu metu nurodomas švietimo trūkumas ir inovacinės kultūros stoka institucijose. Matomas atotrūkis tarp mokslinės literatūros pateikiamų bei praktikoje taikomų algoritminių sprendimų, tam įtakos gali turėti daug veiksnių: minėtas žinių trūkumas apie galimą DI įdarbinimą, nepasitikėjimas technologijomis, įvairūs stabdžiai, kaip finansai, duomenų apsauga (itin jautrius duomenis turinti sritis), specialistų trūkumas. Lietuvos viešajame sektoriuje šių technologijų adaptacija kol kas lėta, interviu pradžiose tiek mokslininkai, tiek specialistai pripažįsta menkai žinantys konkrečių antikorupcijai skirtų algoritminių įrankių – tiek dėl žinių, suvokimo stokos, tiek dėl komunikacijos trūkumo, kadangi nemažai iniciatyvų vyksta izoliuotai ir nėra viešai prieinamos. Šioje vietoje susiduriama su Lietuvos valstybinių institucijų charakteristiniu bruožu – komunikacija yra tik formali, dažniausiai visuomenei pateikiama tik būtina informacija, kuri orientuota į gero institucijų įvaizdžio kūrimą. Aiški ir atvira komunikacija apie naudojama DI gali sutrikdyti visuomenės pasitikėjimą, sukelti papildomų abejonių institucijų veiklos rezultatais. Darytina išvada, jog įstaigos pasirenka neskelbti tokio pobūdžio informacijos arba apsiriboti gan paviršutiniškais pranešimais.

Interviu metu atsiskleidę iššūkiai, trukdantys diegti algoritmines technologijas – daugialypiai. Specialistai akcentuoja žmogiškųjų išteklių stoką: sunku rasti ir pritraukti specialistus, kurie apmokytų darbui su DI sistemomis ir padėtų jas diegti institucijos viduje, o pačių darbuotojų motyvacija mokytis naujų darbo metodų – menka. Tai siejasi ir su finansinių resursų stoka, kadangi biudžetinėse įstaigose finansų kiekis yra ribotas, tai stabdo inovacijų plėtrą. Tyrimo metu paminėtas

nesėkmingas „SauleIS“ projektas, pasak specialistų nebuvo užbaigtas dėl tiekėjų klaidų, tai nurodo kitą riziką, kai net ir skiriant lėšas, projektai gali nebūti išpildyti dėl išorinių veiksnių. Tai veda prie „užburto rato“ – inovacijoms diegti stinga specialistų kompetencijų bei finansų, o nesant sėkmingų rezultatų/ pavyzdžių sunku pagrįsti didesnių investicijų poreikį. Duomenų prieiga ir kokybė – tai dar vienas kylantis iššūkis, kuris pagal analizuotą mokslinę literatūrą turi tiesioginį poveikį algoritmų efektyvumui. Lietuvoje tam tikrų registrų informacija yra „parduodama“, net ir teisėsaugos institucijoms, o nevyriausybinėms organizacijoms dėl mažesnių resursų ir veiklos pobūdžio prieiga prie šių duomenų dar sudėtingesnė. Šioje srityje atsiskleidė požįriui skirtumai tarp tiriamų grupių, mokslininkai buvo daugiau susirūpinę duomenų kokybės aspektais (pvz.: savideklaracijų patikimumas), jų atvėrimu, o specialistai daugiau minėjo duomenų apsaugą bei kibernetinio saugumo svarbą. Tokie rezultatai sufleruoja, kad specialistai neturi bazinių žinių apie sistemų veikimo principus – jei sistemos trūks duomenų arba jie bus nekokybiški, sistema darys klaidas, bus šališka, diskriminacinė. Šia mintį galime sieti ir su teorine dalimi, kurioje nurodoma, kad net ir turint sistemas – specialistams būtina suprasti sistemos funkcionalumą bei veikimo metodus, tam kad galėtų tinkamai taikyti sistemų teikiamus rezultatus.

Teorijoje aptarti DI etikos principai bei DI aktas turėtų suteikti ne tik gaires bet ir nustatyti aiškias taisykles saugiam ir atsakingam technologijų naudojimui. Tačiau empiriniai duomenys rodo, kad šios gairės dar nėra pakankamai įsiliesios į praktiką – reta ES šalių publikacija/ projektas viešai deklaruoja etikos principų laikymąsi. Interviu analizės metu tarp mokslininkų ir specialistų išryškėjo didelė atskirtis DI etikos principų bei DI reguliavimo suvokime. Specialistai yra menkai susipažinę su DI etikos gairėmis, rekomendacijomis ar net DI aktu – dauguma jų vadovaujasi paviršutinišku požįriu – siekdami gerų veiklos rezultatų ir mano, jog asmeninė atsakomybė ir duomenų apsaugos laikymasis yra pakankamas atsakingo naudojimo pagrindas. Tuo tarpu mokslininkai nors ir sutaria dėl DI etikos principų neveiksmingumo apsaugant nuo galimų rizikų, nurodo jų svarbą, kaip visa ko pagrindą, nes šie principai turi būti naudojami algoritminių technologijų kūrimo procese ir reglamentavimo rengime. Mokslininkai taip pat sutaria dėl DI reguliavimo (DI akto) reikalingumo, tačiau nurodo jo esamus trūkumus, neaiškumus, keblumus bandant taikyti jį praktikoje. Tuo tarpu specialistai orientuoti į greitą ir lengvą technologijų panaudojimą darbe, nors ir nėra susipažinę su DI aktu, išreiškia susirūpinimą dėl per griežto reguliavimo. Specialistai taip pat mini BDAR sukuriamus sunkumus, dėl duomenų privatumo, jų naudojimo, o kai kuriems iš šios grupės tiriamųjų, tai tampa, kaip priežastis netaikyti algoritminių sistemų. Viso darbo rėmuose aptarta informacija rodo, kad technologijų įdiegimas be atitinkamo reguliavimo ir kontrolės gali sukurti naujų rizikų, o perdėtas atsargumas ir žinių stoka gali palikti neišnaudotą šių technologijų potencialą.

Apibendrinant, galima tvirtai teigti, jog algoritminiai įrankiai yra veiksmingiausi bei daugiausiai naudojami, kai šalyje ar institucijų viduje yra suformuota aiški DI politika, suformuotos taisyklės bei skatinamos inovacijos. Tiek teorinė, tiek empirinė tyrimo dalis parodė, jog šios priemonės prisideda prie korupcinio pobūdžio veikų išaiškinimo bei nelegalios veikos apraiškų identifikavimo. Tuo pačiu, empirinis tyrimas atskleidė, jog be organizacinio pasirengimo, skiriamų išteklių bei specialistų švietimo šių technologijų potencialas liks neišvystytas – pati technologija savaime nėra panacėja. Nors žmogiškojo faktoriaus klaidos ir yra apribojamos, jos neišnyksta, o tik keičia formą – žmogus turi tapti technologijų prižiūrėtoju ir valdytoju, kuriam būtina suvokti įrankio veikimą, jo galimą šališkumą ar daromas klaidas. Lietuvoje algoritminių technologijų taikymas antikorupcinėje veikloje, nors ir lėtas, tačiau yra besivystantis ir ganėtinai pageidaujamas procesas. Tam spartinti būtina stiprinti kompetencijas, DI teisinį ir etinį aiškumą bei tarpinstitucinį ir tarptautinį bendradarbiavimą. Galiausiai ES pavyzdžiai bei teorijoje pateikti DI taikymo modeliai suponuoja neišvengiamą algoritmų taikymą antikorupcinėje veikloje, tačiau efektyviam jų diegimui bei naudojimui būtina įtvirtinti tinkamą jų kontrolę, priežiūrą bei stiprinti Lietuvoje matomas šios srities spragas.

Išvados

1. Teorinė dalis parodė, jog įvairaus tipo algoritminės technologijos gali padėti aptikti korupcijos rizikas, užkirsti kelią žmogiškojo faktoriaus daromoms manipuliacijoms bei didinti institucijų efektyvumą. Tačiau reiktų atkreipti dėmesį, jog šių technologijų nauda bei potencialas gali būti įgyvendintas tik turint aiškius kontrolės mechanizmus, bei tinkamai diegiant ir naudojant sistemas – kitu atveju sistemos gali būti šališkos, daryti klaidas (Nyderlandų ir Danijos pavyzdys) ar net būti panaudotos korupciniais veiksmais atlikti.

2. Tiek literatūros analizė, tiek ES šalių patirtys bei interviu duomenys atskleidė, kad būtent viešieji pirkimai yra daugelio inovacijų fokusas, siekiant aptikti anomalijas, rizikos veiksnius, neskaidrius susitarimus, interesų konfliktus. Taip pat svarbi sritis išlieka finansų sektoriaus kontrolė su siekiu stebėti bei nustatyti mokestinį sukčiavimą, neteisėtą praturtėjimą, kuris dažnu atveju gali sietis su korupcinėmis veikomis.

3. Dokumentų analizė apie ES šalių naudojamas sistemas nurodo, kad duotuoju momentu, tai gan plačiai taikomos sistemos antikorupcinei aplinkai stiprinti. Verta pabrėžti, jog duomenų prieiga stipriai priklauso nuo šalių komunikacijos atvirumo, tačiau būtent tinkama komunikacija gali tapti puikia prevencine priemone.

4. Lietuvoje šių inovacijų plėtra lėta bei apsunkinama įvairių iššūkių. Pažangiausios institucijos tyrimo rėmuose ganėtinais plačiai naudojasi generatyviniu DI, o aukštos rizikos sistemų kūrimas bei diegimas yra tik pirmuosiuose projektų etapuose.

5. Specialistai susiduria su finansų, specialistų bei žinių stoka. Šios problemos sukuria „užburtą ratą“ – be finansų ar žinių, sunku pasamdyti specialistus ar mokyti savus, sistemų kūrimo ir jų taikymo, o be sistemų naudojimo sunku parodyti rezultatą, kuris galėtų pagrįsti didesnę finansavimą.

6. Empirinio tyrimo duomenys, nurodo nemažą atotrūkį tarp mokslo ir praktikos – tai patvirtina ir literatūros analizė. Mokslininkai turi įdomesnių prieigų, kaip būtų galima įdarbinti algoritmines sistemas, taip pat nepritaria jog DI etikos principai gali apsaugoti nuo rizikų, įprasmina jas – kaip visa ko pagrindą. Taip pat DI aktas, šios grupės, nurodomas, kaip reikalingas, tačiau nesuteikiantis didelio aiškumo ir sunkiai pritaikomas praktikoje. Tuo tarpu specialistai yra orientuoti į greitą naudos gavimą, todėl technologijos yra naudojamos administracinėms, monotoniškoms užduotims atlikti (mažai žinių apie DI pritaikomumą). Taip pat ši grupė nebuvo pakankamai susipažinusi su DI etikos principais bei DI aktu, tačiau turėjo gan tvirta nuomone, jog reguliavimas neturėtų būti griežtas, nes tai stabdo inovacijas.

7. Pastebėta, kad įtaką sistemų nenaudojimui gali daryti žinių trūkumas apie DI bei motyvacijos stoka gilintis į esamą jo reguliavimą – tai tampa pretekstu nesinaudoti sistemomis.

Specialistai linkę argumentuoti, jog esantys įstatymai (pvz.: BDAR) suvaržo duomenų pritaikomumą, o algoritminės technologijos kelia riziką duomenų saugumui, privatumui.

Apibendrinant, algoritminių įrankių vaidmuo antikorupcinėje veikloje auga, tačiau jų sėkmei būtina kompleksinė prieiga: specialistų rengimas, mokymas, aiškūs reguliavimo principai ir politinė strategija. Tik turint kokybišką suvokimą, kontrolę bei priežiūrą šios sistemos gali pozityviai prisidėti prie antikorupcinės aplinkos stiprinimo.

Rekomendacijos

Rekomendacijos skirtos visoms viešojo sektoriaus institucijoms/ organizacijoms, kurios prisideda prie antikorupcinės aplinkos gerinimo bei siekia inovacinių sprendimų padėsiančių spartinti jų veiklos procesus.

- Svarbus tarpinstitucinis ir tarptautinis bendradarbiavimas, orientuotas į informacijos, gerųjų praktikų mainus bei bendrų projektų (pvz.: dvynių projektai, kai į pažengusios šalies institucijas yra išsiunčiamas asmuo iš mažiau pažengusiosios, tam kad per skirtą laiką būtų suteikiamos visos žinios apie įdiegtas bei pasiteisinusias algoritmines technologijas antikorupcinei aplinkai gerinti) įgyvendinimą.

- Institucijoms būtina ne tik komunikuoti tarpusavyje, bet ir su visuomene, apie tai kokios algoritminės technologijos yra naudojamos darbo procesuose (neturima omenyje tų sistemų, kurios neviešinamos dėl slaptos institucinės veiklos). Institucijos turėtų, visuomenei patogiais kanalais, teikti pranešimus apie tai kokiomis etikos gairėmis vadovaujamosi diegiant bei naudojant sistemas, kokie taikomi apsaugos mechanizmai. Tinkamas informacijos pateikimas gali veikti, kaip efektyvi prevencijos priemonė.

- Politikos formuotojai bei viešojo sektoriaus institucijos, kurios siekia naudoti algoritmines technologijas, turi suformuoti aiškią organizacijų kryptį orientuota į inovacijas, reglamentuoti DI taikymo principus ir skatinti inovacijoms palankią organizacinę kultūrą, t.y. kurti vidines DI naudojimosi gaires, DI etikos kodeksus, paskirti padalinį, komandą ar specialistą atsakingą už DI diegimo, naudojimosi ir priežiūros procesus, apdovanoti DI iniciatyvas, kurios buvo veiksmingiausios gerinant antikorupcinę aplinką, sukurti vidinę „testavimo aplinką“, kur būtų galima saugiai išbandyti bei eksperimentuoti algoritminius sprendimus.

- Šiame kontekste, viešojo sektoriaus specialistai, turi būti ne tik supažindinti su DI etikos principais bei teisiniu reguliavimu, bet ir tinkamai apmokyti praktiniam darbui su šiomis technologijomis. Būtina rengti mokymus, kuriuose specialistams būtų suteikiamos žinios apie teisinį šių technologijų reguliavimą, tobulinami praktiniai DI rizikų atpažinimo ir valdymo

įgūdžiai, mokymai su realiais pavyzdžiais (viena iš galimų priemonių – sukurta vidinė arba viešojo sektoriaus darbuotojams skirta mokymų platforma, kurių pabaigoje asmuo atlieka žinių testą ir įgyja sertifikatą). Sisteminiis švietimas padės išvengti potencialių rizikų ir žalų.

- Bendradarbiavimas su mokslo bendruomene, šioje srityje, gali būti itin efektyvi priemonė, siekiant įdarbinti turimus duomenis (privačių interesų registras, lobistų sąrašas, viešųjų pirkimų duomenys), kurti inovatyvius, algoritminių įrankių skirtų antikorupciniam darbui, sprendimus bei mažinti atotrūkį tarp mokslo ir praktikos. Siekiant pažangos, būtina, kad antikorupcinės srities specialistų praktika bent iš dalies siektų vyti DI mokslininkų generuojamas algoritminių technologijų prieigas darbui prieš korupciją.

Literatūra

1. Adam, I., & Fazekas, M. (2021). Are emerging technologies helping win the fight against corruption? A review of the state of evidence. *Information Economics and Policy*, 57. <https://doi.org/10.1016/j.infoecopol.2021.100950>
2. Adobor, H., & Yawson, R. (2022). The promise of artificial intelligence in combating public corruption in the emerging economies: A conceptual framework. *Science and Public Policy*. <https://doi.org/10.1093/scipol/scac068/6889870>
3. Albert Sanchez-Graells. (2021). Procurement corruption and artificial intelligence: between the potential of enabling data architectures and the constraints of due process requirements.
4. Aldana, A., Falcón-Cortés, A., & Larralde, H. (2022). A machine learning model to identify corruption in México's public procurement contracts.
5. Asaro, P. M. (2019) 'AI ethics in predictive policing: From models of threat to an ethics of care', *IEEE Technology and Society Magazine*, 38(2), p. 40–53.
6. Berryhill, J. et al. (2019) 'Hello, World: Artificial Intelligence and its use in the Public Sector', *OECD Observatory of Public Sector Innovation (OPSI)*, 36.
7. Calo, R. (2017). *Artificial Intelligence Policy: A Primer and Roadmap*. <https://www.>
8. Casey, D., Burrell, P. ir Sumner, N. (2019) 'Decision Support Systems in Policing.', *European Law Enforcement Research Bulletin*, 4, p. 97
9. Ceva, E., & Jiménez, M. C. (2022). Automating anticorruption? *Ethics and Information Technology*, 24(4). <https://doi.org/10.1007/s10676-022-09670-x>
10. Ceva, E., & Jiménez, M. C. (2022). Automating anticorruption? *Ethics and Information Technology*, 24(4). <https://doi.org/10.1007/s10676-022-09670-x>
11. Coalition For Integrity. (2021). *Using Machine Learning For Anti-Corruption Risk And Compliance*. www.coalitionforintegrity.org
12. Dincer, O., & Johnston, M. (2020). Legal corruption? *Public Choice*, 184(3–4), 219–233. <https://doi.org/10.1007/s11127-020-00832-3>
13. Dobrovolska, O., & Rozhkova, M. (2024). The Impact of Digital Transformation on the Anti-Corruption and Cyber-Fraud System. *Business Ethics and Leadership*, 8(3), 231–252. [https://doi.org/10.61093/bel.8\(3\).231-252.2024](https://doi.org/10.61093/bel.8(3).231-252.2024)

14. Europos komisija (2020) 'White Paper on Artificial Intelligence: a European approach to excellence and trust'. Internetinė prieiga: https://commission.europa.eu/publications/whitepaper-artificial-intelligence-european-approach-excellence-and-trust_e
15. Europos parlamentas (2020) 'Artificial Intelligence and Law Enforcement Impact on Fundamental Rights'.
16. Europos Sąjungos Taryba. (2024). Artificial Intelligence Act.
17. Europos taryba (2018) 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions Fostering a European approach to Artificial Intelligence', p. 29–50.
18. Europos veiksmingo teisingumo komisija (CEPEJ) (2018) 'European ethical charter on the use of Artificial Intelligence in judicial systems and their environment', Adopted at the 31st Plenary Meeting of the CEPEJ
19. Fazekas, M. (2017). Uncovering high-level corruption: Cross-national objective corruption risk indicators using public procurement data. Article in British Journal of Political Science. <https://doi.org/10.17863/CAM.12545>
20. Guillaume Nicaise, & Daniel Sejerøe Hausenkamph. (2025). Unlocking AI's potential in anti-corruption: Hype vs. Reality. <https://www.u4.no/blog/unlocking-ai-s-potential-in-anti-corruption-hype-vs-reality>
21. Hagendorff, T. (2020). The Ethics of AI Ethics: An Evaluation of Guidelines. *Minds and Machines*, 30(1), 99–120. <https://doi.org/10.1007/s11023-020-09517-8>
22. Hagendorff, T. (2022). Blind spots in AI ethics. *AI and Ethics*, 2(4), 851–867. <https://doi.org/10.1007/s43681-021-00122-8>
23. Hongladarom, S., & Bandasak, J. (2024). Non-western AI ethics guidelines: implications for intercultural ethics of technology. *AI and Society*, 39(4), 2019–2032. <https://doi.org/10.1007/s00146-023-01665-6>
24. Ibarra, G., Douglas, D. M. ir Tharmarajah, M. (2020) 'Machine Learning and Responsibility in Criminal Investigation', Australia's National Science Agency.
25. Yeferson Torres Berru, Vivian Félix López Batista, Pablo Torres-Carrión, and, & Maria Gabriela Jimenez. (2020). Artificial Intelligence Techniques to Detect and Prevent Corruption

- in Procurement: A Systematic Literature Review (M. Botto-Tobar, M. Zambrano Vizuite, P. Torres-Carrión, S. Montes León, G. Pizarro Vásquez, & B. Durakovic, Eds.; Vol. 1194). Springer International Publishing. <https://doi.org/10.1007/978-3-030-42520-3>
26. ISO 42001 Informacinės technologijos. Dirbtinis intelektas. <https://www.isosertifikatas.lt/iso-42001>
 27. Issar, S., & Aneesh, A. (2022). What is algorithmic governance? *Sociology Compass*, 16(1). <https://doi.org/10.1111/soc4.12955>
 28. Jakhar, D. ir Kaur, I. (2019) 'Artificial intelligence, machine learning and deep learning: definitions and differences', *Clinical and Experimental Dermatology*, 45(1), p. 131–132.
 29. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, 37(3). <https://doi.org/10.1016/j.giq.2020.101493>
 30. Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy Artificial Intelligence. *Government Information Quarterly*, 37(3). <https://doi.org/10.1016/j.giq.2020.101493>
 31. Jenkins, M., Vrushi, J., Wriedt, L., & Eriksson, D. (2022). The corruption risks of artificial intelligence. www.transparency.org
 32. Jobin, A., Ienca, M. ir Vayena, E. (2019) 'The global landscape of AI ethics guidelines', *Nature Machine Intelligence*, 1(9), p. 389–399.
 33. Kayikci, S., & Khoshgoftaar, T. M. (2024). Blockchain meets machine learning: a survey. *Journal of Big Data*, 11(1). <https://doi.org/10.1186/s40537-023-00852-y>
 34. Köbis, N., Starke, C., & Rahwan, I. (2021). Artificial Intelligence as an Anti-Corruption Tool (AI-ACT) Potentials and Pitfalls for Top-down and Bottom-up Approaches.
 35. Köbis, N., Starke, C., & Rahwan, I. (2022). The Promise and Perils of using Artificial Intelligence to fight Corruption.
 36. Kossow, N., Windwehr, S., Jenkins, M., Eriksson, D., Vrushi, J., & Millar, L. (2021). Algorithmic transparency and accountability.
 37. Larsson, S. (2020). On the Governance of Artificial Intelligence through Ethics Guidelines. In *Asian Journal of Law and Society* (Vol. 7, Issue 3, pp. 437–451). Cambridge University Press. <https://doi.org/10.1017/als.2020.19>

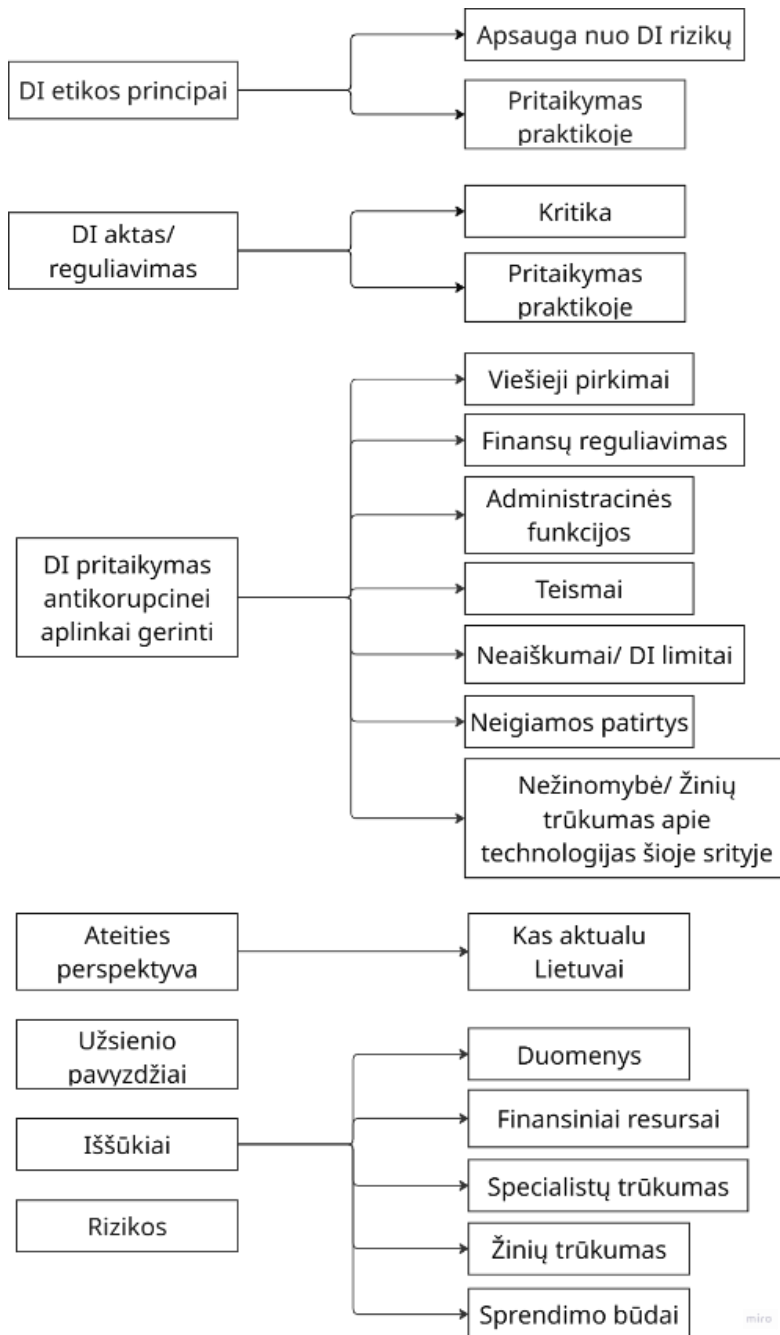
38. Law Business Research Ltd. (2021). Global data review insight handbook. www.globaldatareview.com
39. Leib, M., Köbis, N. C., Rilke, R. M., Hagens, M., & Irlenbusch, B. (2021). The corruptive force of AI-generated advice.
40. Lessig, L. (2013). "Institutional Corruption" Defined.
41. Lima, M. S. M., & Delen, D. (2020). Predicting and explaining corruption across countries: A machine learning approach. *Government Information Quarterly*, 37(1). <https://doi.org/10.1016/j.giq.2019.101407>
42. Lyuben, A. et al. (2021) Predictive Policing in the Belgian Police Service.
43. López-Iturriaga, F. J., & Sanz, I. P. (2018). Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. *Social Indicators Research*, 140(3), 975–998. <https://doi.org/10.1007/s11205-017-1802-2>
44. Meijer, A. ir Wessels, M. (2019) 'Predictive Policing: Review of Benefits and Drawbacks', *International Journal of Public Administration*, 42(12), p. 1031–1039.
45. Mittelstadt, B. (2019). Principles alone cannot guarantee ethical AI.
46. Nathalie A. Smuha. (n.d.). The Cambridge Handbook of THE LAW, ETHICS AND POLICY OF ARTIFICIAL INTELLIGENCE.
47. National Telecommunications and Information Administration (2024) „FACT SHEET: NTIA Urges Policy Changes to Boost Accountability and Trustworthiness in Artificial Intelligence Systems“ United States Department of Commerce. <https://www.ntia.gov/other-publication/2024/fact-sheet-ntia-artificial-intelligency-policy-accountability>
48. Odilla, F. (2023). Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. *Crime, Law and Social Change*, 80(4), 353–396. <https://doi.org/10.1007/s10611-023-10091-0>
49. Odilla, F. (2024). Unfairness in AI Anti-Corruption Tools: Main Drivers and Consequences. *Minds and Machines*, 34(3). <https://doi.org/10.1007/s11023-024-09688-8>
50. Pagano, T. P., Loureiro, R. B., Lisboa, F. V. N., Peixoto, R. M., Guimarães, G. A. S., Cruz, G. O. R., Araujo, M. M., Santos, L. L., Cruz, M. A. S., Oliveira, E. L. S., Winkler, I., & Nascimento, E. G. S. (2023). Bias and Unfairness in Machine Learning Models: A Systematic Review on Datasets, Tools, Fairness Metrics, and Identification and Mitigation Methods. In

51. Parycek, P., Schmid, V., & Novak, A. S. (2024). Artificial Intelligence (AI) and Automation in Administrative Procedures: Potentials, Limitations, and Framework Conditions. *Journal of the Knowledge Economy*, 15(2), 8390–8415. <https://doi.org/10.1007/s13132-023-01433-3>
52. Per Aarvik. (2019). Artificial Intelligence - a promising anti-corruption tool in development settings? <https://www.flickr.com/photos/artbystevejohnson/>
53. Per Aarvik. (2020). Blockchain as an anticorruption tool.
54. Petheram, A., Pasquarelli, W., & Stirling, R. (2019). The Next Generation of Anti-Corruption Tools: Big Data, Open Data & Artificial Intelligence. <https://fullfact.org/health/spending-english-nhs/>
55. Poltoratskaia, V., & Fazekas, M. (2024). Data analytics for anti-corruption in public procurement. In *Routledge Handbook of Public Procurement Corruption* (pp. 42–59). Taylor and Francis. <https://doi.org/10.4324/9781003220374-6>
56. Rabuzin, K. and Modrušan. N. (2019). Prediction of Public Procurement Corruption Indices using Machine Learning Methods.
57. Sandra Wachter. (2024). Limitations and Loopholes in the EU AI Act and AI Liability Directives: What This Means for the European Union, the United States, and Beyond. *Yale Journal of Law & Technology*, Volume 26(Issue 3).
58. Sarker, I. H., Mohammad, N., Janicke, H., Watters, P., & Nepal, S. (2023). AI Potentiality and Awareness: A Position Paper from the Perspective of Human-AI Teaming in Cybersecurity. <https://doi.org/10.48550/arXiv.2310.12162>
59. Segun, S. T. (2021). Critically engaging the ethics of AI for a global audience. *Ethics and Information Technology*, 23(2), 99–105. <https://doi.org/10.1007/s10676-020-09570-y>
60. Selmy, H.A., Mohamed, H.K., Medhat, W., 2024. Big data analytics deep learning techniques and applications: A survey. *Inf. Syst.* 120, 102318. <https://doi.org/10.1016/j.is.2023.102318>
61. Sommersguter-Reichmann, M., Wild, C., Stepan, A., Reichmann, G., & Fried, A. (2018). Individual and Institutional Corruption in European and US Healthcare: Overview and Link of Various Corruption Typologies. In *Applied Health Economics and Health Policy* (Vol. 16, Issue 3, pp. 289–302). Springer International Publishing. <https://doi.org/10.1007/s40258-018-0386-6>

62. Szreder, M. (2022). Noise and bias – some controversies raised by the book ‘Noise: A Flaw in Human Judgment’, written by Daniel Kahneman, Olivier Sibony, Cass R. Sunstein. *Przegląd Statystyczny*, 69(1), 39–49. <https://doi.org/10.5604/01.3001.0015.8792>
63. Taeihagh, A. (2021). Governance of artificial intelligence. *Policy and Society*, 40(2), 137–157. <https://doi.org/10.1080/14494035.2021.1928377>
64. Transparency international. (2023). CORRUPTION PERCEPTIONS INDEX 2023. www.transparency.org/cpi
65. U4 anticorruption resource center (2025) „Unlocking AI’s potential in anti-corruption: Hype vs. Reality“ <https://www.u4.no/blog/unlocking-ai-s-potential-in-anti-corruption-hype-vs-reality>
66. UNESCO (2021) The Ethics of Artificial Intelligence.
67. UNICRI ir INTERPOL (2020) ‘Towards Responsible AI innovation. Second INTERPOL - UNICRI report on artificial intelligence for law enforcement’.
68. Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, 21(7), 1076–1100. <https://doi.org/10.1080/14719037.2018.1549268>
69. Wirtz, B. W., & Müller, W. M. (2019). An integrated artificial intelligence framework for public management. *Public Management Review*, 21(7), 1076–1100. <https://doi.org/10.1080/14719037.2018.1549268>
70. Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly*, 39(4). <https://doi.org/10.1016/j.giq.2022.101685>
71. Wirtz, B. W., Weyerer, J. C., & Kehl, I. (2022). Governance of artificial intelligence: A risk and guideline-based integrative framework. *Government Information Quarterly*, 39(4). <https://doi.org/10.1016/j.giq.2022.101685>
72. Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3). <https://doi.org/10.1016/j.giq.2021.101577>
73. Zuiderwijk, A., Chen, Y. C., & Salem, F. (2021). Implications of the use of artificial intelligence in public governance: A systematic literature review and a research agenda. *Government Information Quarterly*, 38(3). <https://doi.org/10.1016/j.giq.2021.101577>

74. Žemgulytė, D., Muravjovas, S., Semionovaitė, E., Kalinauskienė, I., & Aleksandravičius, L. (2023). Beieškant dirbtinio intelekto viešajame sektoriuje. www.skaidrumas.lt
75. Žydzūnaitė, V., Sabaliauskas, S. (2017). Kokybiniai tyrimai: principai ir metodai: vadovėlis socialinių mokslų studijų programų studentams. Vilnius: Vaga. <https://hdl.handle.net/20.500.12259/57984>

1 priedas „Kodų ir subkodų medis“



2 priedas “ES šalių naudojamos algoritminės technologijos antikorupcinei aplinkai gerinti“

	Šalys	Sistema/ pavadinimas	Paskirtis	Šaltinis
1	Austrija	DI/ MM	Prognostinės analizės kompetencijos centras (PACC), specialus Finansų ministerijos padalinys, naudoja prognozavimo analizę ir dirbtinį intelektą, kad nustatytų mokesčių slėpimą ir identifikuotų konkrečius verslininkus bei asmenis. PACC taiko pažangius prognozavimo analizės ir mašininio mokymosi metodus, kurie padėjo padidinti papildomas mokestines pajamas taikant audito priemones ir nustatyti fizinius bei juridinius asmenis, kurie nesilaikė reikalavimų, o tai taip pat padeda aptikti ir piktnaudžiavimo atvejus.	https://www.bmf.gv.at/en/press/press-releases/2024--New/August-2024/BMF-generated-around-EUR-185-million-in-tax-income-from-AI-in-2023-.html
		Algoritmai	Austrijoje jauniems tėvams nereikia teikti prašymų išmokoms už vaikus gauti; vietoj to, atsakinga agentūra automatiškai gauna ir apdoroja atitinkamą informaciją po vaiko gimimo ir automatiškai perveda lėšas. Šiuo būdu yra apeinamas nebūtinamas kontaktas su asmeniu, kuris gali kelti korupcinio pobūdžio ar neskaidrumo rizikas.	https://www.bmf.gv.at/en/topics/taxation/family-and-children/family-allowance.html
		DI/ ML „VATCalc“	Austrijos DI padalinys pasiekė pozityvių rezultatų kovodamas su mokesčių mokėtojų sukčiavimu dėl PVM. Mokesčių institucijos prisidėjo prie skaidrumo taikant šias pažangias technologijas, kad galėtų veiksmingiau nustatyti sukčiavimo atvejus.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
2	Belgija	Algoritmai	Belgijoje, siekiant sudaryti daugiau lygių galimybių, algoritminė sistema padeda paskirstyti mokinius į mokyklas. Iki algoritmo įdiegimo mokyklos mokinius registruodavo pagal taisyklę "kas pirmas, tas pirmas". Ši sistema gali eliminuoti piktnaudžiavimo terpę papirkinėjimui dėl vietos mokyklose bei tokiu būdu skaidrina bei gerina viešąsias paslaugas.	https://knowledgehub.transparency.org/assets/uploads/kproducts/Algorithmic-Transparency_2021.pdf https://automatingsociety.algorithmwatch.org/report2020/belgium/belgium-story/

		Blokų grandinės technologija (ang. Blockchain)	Antverpeno IT agentūra "Digipolis" kartu su projekto partnere "BallistiX" kuria blokų grandinę pagrįstą taikomąją programą, kuri leis paskelbti užklausą dėl pasiūlymo, pateikti ir atverti pasiūlymus. Manoma, kad blokų grandinės naudojimas užtikrins kiekvieno viešųjų pirkimų proceso etapo patikimumą, nes jie bus registruojami skaidriai.	https://ec.europa.eu/assets/grow/growth/_toolbox/pp-emerging-tech/tabledet.html?d=11
		Algoritmai	MEDIAAN leidžia matyti ir analizuoti istorines prekių ir paslaugų kainas, o šie duomenys itin naudingi viešųjų pirkimų procese. Platformoje yra kainų peržiūros programa, pusiau automatinis kainų apskaičiavimas bei vienetinių ir valandinių įkainių apskaičiavimas. Šie duomenys taip pat gali būti naudojami sudėtingesniems algoritmams apmokyti.	https://www.vlaanderen.be/medium-voor-economische-data-informatie-en-applicaties-over-overheidsopdrachten-mediaan
		DI/ ML „VATCalc“	Nuo 2026 m. sausio mėn. pradedama taikyti e. sąskaitų faktūrų išrašymo pareiga, kuri prisideda prie didesnio finansinio skaidrumo ir PVM reikalavimų laikymosi. Sistema užtikrina, kad sandorių duomenys būtų automatiškai standartizuoti, skaitmeniniu būdu atsekami ir jais būtų saugiai keičiamasi.	https://www.vatcalc.com/belgium/belgium-b2b-e-invoicing-july-2024-update/
		„V-ICT-OR“ Blokų grandinės projektas	V-ICT-OR (Flandrijos vietos valdžios institucijų IRT ir informacijos valdymo srityje dirbančių asmenų narystės organizacija) kartu su „Digipolis“ paskelbė viešųjų pirkimų blokų grandinės sprendimų paiešką. Projektas buvo naudojamas kaip būdas susipažinti su nauju viešųjų pirkimų proceso organizavimo būdu.	https://v-ict-or.be/ https://www.vlaio.be/en/vlaio-network/programme-innovation-procurement-pip/buyit-public-joint-digital-purchasing-platform
3	Bulgarija	AI/ didieji kalbos modeliai (ang. large language model) „BgGPT“	Igyvendinant BgGPT Nacionalinei pajamų agentūrai, buvo įdiegta funkcija, kuri padeda rasti tikslus pokalbių roboto atsakymų šaltinius, todėl darbuotojai gali lengvai patikrinti informaciją. Tai ne tik padeda sumažinti klaidų skaičių, bet ir didina visuomenės pasitikėjimą automatizuotomis sistemomis. Šis sprendimas didina viešųjų paslaugų skaidrumą ir patikimumą.	https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/open-source-ai-bulgaria-insaits-bggpt-can-foster-public-and-private-sector-innovation

		Blokų grandinės technologija	Bulgarijos savivaldybei buvo sukurta blokų grandinė, kuri tarnautų kaip tam tikra savivaldybių grupės prekyvietė. Pagal šią sistemą automatiškai būtų atliekamas konkurso užklauso reikalavimų ir tiekėjo pasiūlymo atitikimas. Kvalifikavimo / diskvalifikavimo procesas gali būti automatizuotas ir pirkėjas negalės matyti kainos pasiūlymo, jei tiekėjas bus diskvalifikuotas. Sistema suteikia galimybę užtikrinti viešųjų pirkimų proceso skaidrumą.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en
4	Čekija	-	-	-
5	Danija	DI	Danijos socialinės rūpybos institucija Udbetaling Danmark (UDK) naudojo dirbtinio intelekto priemones, kad nustatytų sukčiavimo socialinėmis išmokomis atvejus. Ši sistema neproporcingai veikė marginalizuotas grupes, įskaitant neįgaliuosius, mažas pajamas gaunančius asmenis, migrantus, pabėgėlius ir rasines mažumas. Taikant dirbtiniu intelektu grindžiamą metodą renkami išsamūs duomenys, apimantys gyvenamosios vietos statusą, pilietybę, gimimo vietą ir šeiminius santykius	https://www.amnesty.org/en/documents/eur18/8709/2024/en/ https://www.amnesty.org/en/latest/news/2024/11/denmark-ai-powered-welfare-system-fuels-mass-surveillance-and-risks-discriminating-against-marginalized-groups-report/
		Blokų grandinės technologija „Tradeshift“	"Tradeshift" yra pasaulinė tiekimo grandinės mokėjimų ir prekyviečių lyderė, siūlanti skaitmeninę platformą, kuri sujungia pirkėjus, tiekėjus ir finansų įstaigas, kad būtų supaprastinti tiekimo grandinės procesai. Siekiama optimizuoti verslo sandorių efektyvumą ir skaidrumą, e. sąskaitų faktūrų išrašymą, viešuosius pirkimus, tiekėjų valdymą ir finansinių paslaugų integraciją.	https://tech.eu/2024/06/20/denmark-europes-hub-for-tech-innovation-and-collaboration/
6	Estija	Blokų grandinės technologija „KSI Blockchain“	Estija naudoja Keyless Signature Infrastructure (KSI) Blockchain technologiją, kad užtikrintų savo duomenų vientisumą ir saugumą. Šis blokų grandinės sprendimas suteikia veiksmingą būdą skaitmeninių įrašų autentiškumui patikrinti, taip didinant pasitikėjimą e. valdžios paslaugomis. Estija, skaitmenizavo beveik visas savo viešąsias paslaugas - nuo mokesčių mokėjimo iki verslo registravimo, taip užtikrindama didesnę skaidrumą ir apsunkindama galimybę korumpuotiems pareigūnams reikalauti kyšių.	https://e-estonia.com/solutions/cyber-security/ksi-blockchain/ https://www.project-syndicate.org/commentary/technology-can-help-defeat-corruption-but-requires-strong-legal-frameworks-by-azalina-othman-said-2024-11

		DI	Dirbtinis intelektas padeda agentūroms veiksmingiau nustatyti sukčiavimo atvejus ir sumažinti klaidingų teigiamų rezultatų skaičių (ang. false positive), todėl valstybės tarnautojai gali skirti laiko vertingoms užduotims ir kartu kurti pasitikėjimu grįstus santykius su mokesčių mokėtojais. Šiuo metu ETCB siekia sukurti dirbtiniu intelektu pagrįstą "žmogaus įtraukimo į ciklą" sistemą, kuri ne tik leistų veiksmingiau nustatyti mokestinį sukčiavimą, bet ir laikui bėgant padidintų tikslumą.	https://mindtitan.com/resources/industry-use-cases/ai-use-cases-in-government/
7	Graikija	DI/ MM	Graikija steigia specializuotą dirbtinio intelekto padalinį, kuris naudoja "MyDATA" PVM sandorius sukčiavimui nustatyti.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		DI	2024 m. liepos mėn. Nacionalinė skaidrumo institucija pradėjo kurti integruotą informacinę sistemą, skirtą auditui ir patikrinimams valdyti. Į šią sistemą įtrauktos dirbtinio intelekto priemonės, skirtos audito mechanizms stiprinti, apimančios tokias procedūras kaip skundų vertinimas, turto auditas ir drausminių priemonių stebėseną.	https://en.protothema.gr/2024/07/16/the-national-transparency-authority-in-the-digital-age-enhanced-with-an-artificial-intelligence-tool/
		DI/ MM	Nepriklausomos viešųjų pajamų institucijos naudoja dirbtinį intelektą, kad galėtų analizuoti duomenis iš įvairių šaltinių, įskaitant bankines operacijas ir socialinę žiniasklaidą. Tikslas - aptikti neįprastą elgesį ir neatitikimus teikiant ataskaitas apie pajamas, palengvinant tikslingesnį mokesčių auditą ir sumažinant mokesčių slėpimą. Taip pat naudoja mašininio mokymosi sistemas, įskaitant žiniatinklio nuskaitymo įrankius, kad surinktų duomenis iš e. prekybos ir socialinės žiniasklaidos platformų.	https://taxadmin.ai/country/greece-ai-country-report/ https://www.ekathimerini.com/economy/1227625/ai-utilized-in-battle-against-tax-evasion-in-greece/

		DI „FALCON“	Graikija dalyvauja Europos Komisijos finansuojamame FALCON projekte, kuris prasidėjo 2023 m. rugsėjį. Šioje iniciatyvoje daugiausia dėmesio skiriama duomenų analizės priemonių ir dirbtinio intelekto taikomųjų programų, skirtų kovai su didelio masto korupcija ir organizuotu nusikalstamumu, kūrimui. Projektas skirtas tokioms sritims, kaip sukčiavimas viešųjų pirkimų srityje ir politikoje dalyvaujančių asmenų interesų konfliktai.	https://vcl.itl.gr/projects/fight-against-large-scale-corruption-and-organised-crime-networks/
8	Airija	DI/ MM	Airijos viešosios konsultacijos naudoja įvairaus pobūdžio sistemas dėl PVM sąskaitų faktūrų išrašymo ir ataskaitų teikimo sistemų skaitmeninimo, įskaitant galimą nuolatinės sandorių kontrolės, pvz.: realiuoju laiku teikiamų sąskaitų faktūrų arba e. sąskaitų faktūrų stebėjimą.	https://www.vatcalc.com/global/artificial-intelligence-enhances-vat-item-classification-and-tax-code-selection/ https://www.vatcalc.com/ireland/ireland-consults-on-vat-digital-reporting-and-e-invoicing/
9	Ispanija	DI/ MM	Šiame projekte buvo naudojama viena iš DI šakų - neuroninių tinklų metodas, skirtas prognozuoti viešąją korupciją pagal ekonominius ir politinius veiksnius, naudojant duomenis apie realius korupcijos atvejus.	https://www.researchgate.net/publication/321222117_Predicting_Public_Corruption_with_Neural_Networks_An_Analysis_of_Spanish_Provinces
		Blokų grandinės technologija	Įgyvendindamas projektas, kuriuo siekiama panaudoti blokų grandines siekiant pertvarkyti viešąjį administravimą ir viešųjų paslaugų teikimą. Blokų grandinės bus naudojamos registruojant viešųjų pirkimų konkursuose gautus pasiūlymus ir automatizuotai juos vertinant.	https://www.europapress.es/aragon/noticia-aragon-pionera-apostar-tecnologia-blockchain-integrandose-asociacion-alastria-20180917130921.html
		Blokų grandinės technologija	Blokų grandinės pritaikymas siekiant pagerinti viešuosius pirkimus. Pagrindinis tikslas - sudaryti galimybę registruoti pasiūlymą tinkle, t. y. naudoti jį kaip elektroninę pasiūlymų pateikimo priemonę, privalomą pagal direktyvos 2014/24/ES nuostatas. Papildomas tikslas - padidinti viešųjų pirkimų proceso skaidrumą ir palengvinti (kai įmanoma, automatizuoti) sutarčių sudarymo procesą.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en

10	Italija	DI/ ML „VATCalc“	Italija, kuri bene uoliausiai naudojasi dirbtiniu intelektu mokesčių vengimo nustatymo srityje, praėjusiais metais, naudodama dirbtiniu intelektu pagrįstą duomenų analizę, nustatė daugiau kaip 1 mln. didelės rizikos atvejų. Tai apima ir naujausią algoritmą, pagal kurį kryžminės nuorodos į finansinius duomenis padeda nustatyti mokesčių mokėtojus, kuriems gresia rizika nemokėti mokesčių. Jos algoritmas "VeRa" lygina mokesčių deklaracijas, pajamas, nekilnojamojo turto įrašus, banko sąskaitas ir elektroninius mokėjimus, ieškodamas neatitikimų. Tuomet didelės rizikos mokesčių mokėtojai gauna laišką, kuriame prašoma paaiškinti skirtumus. Kuo daugiau duomenų "VeRa" apdoroja, tuo išmanesnė ji tampa.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		DI/ MM	Įrankis naudojamas po viešųjų pirkimų konkurso. Sistema naudoja mašininį mokymąsi, kad nustatytų paslėptus ryšius tarp viešojo administravimo institucijų ir privačių bendrovių, naudodamasis nestruktūruota informacija (pvz., viešųjų pirkimų pavadinimais) iš atvirų viešųjų pirkimų duomenų.	https://www.slideshare.net/slideshow/machine-learning-on-public-procurement-open-data-the-anac-case-study-fabiana-lanotte/98260307
		DI/ MM	Sistema stebi naudotojų elgesį ir naudoja šiuos pastebėjimus, kad pateiktų rekomendacijas dėl mokymų, katalogo tobulinimo, pasiūlytų naujų sąveikos būdų, nustatytų slaptus susitarimus ir t. t. Naudojama natūralios kalbos ir vaizdų aptikimo gebėjimais, kad nustatytų tokius aspektus, kaip pvz., teisingi produktų kodai. Ji taip pat gali atlikti „ex-post“ analizę, kad suprastų naudotojų elgseną.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en
		DI/ MM	Eksperimentuojama su dirbtinio intelekto galimybėmis, kad, naudodamiesi įvairiais duomenų šaltiniais, suprastų savo naudotojų reakciją į naujus konkursus ir pan. Naudojamas mašininio mokymosi platforma, leidžiančia analizuoti pirkėjų ir tiekėjų nuotaikas, susijusias su „Consip“ platforma. Bandomojo etapo metu renkami ir analizuojami duomenys iš „twitter“ (nes duomenys yra atviri), kad būtų galima greitai gauti grįžtamąjį ryšį apie tai, kaip naudotojai reaguoja į naujus konkursus ir pan. Sistema suteikia teigiamą, neutralią arba neigiamą kategoriją skirtingoms atitinkamose twitter'io žinutėse išreikštomis nuotaikoms.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en
11	Kipras	-	-	-

12	Kroatija	DI	Sukurta viešųjų pirkimų stebėsenos sistema, kuri galėtų aktyviai nustatyti viešųjų pirkimų proceso anomalijas. Šia sistema siekiama didinti skaidrumą ir efektyvumą, analizuojant gausius viešųjų pirkimų bylų duomenis, kad būtų galima aptikti galimus pažeidimus. Pažangi viešųjų pirkimų stebėsenos sistema, pagrįsta teksto gavyba ir subalansuotais rodikliais	https://link.springer.com/chapter/10.1007/978-3-030-83014-4_6?utm_source
13	Vokietija	DI „MaLeFiz“	Juo siekiama patobulinti neteisėtų finansinių srautų aptikimą taikant mašininio mokymosi metodus. Programa „MaLeFiz“ pasitelkia dirbtinį intelektą, kad tiksliau išanalizuotų sandorių duomenis, sumažintų klaidingų pavojaus signalų skaičių ir padėtų nustatyti tikrą įtartiną veiklą. Projekte pabrėžiama, kad AI sprendimai turi būti paaiškinami ir skaidrūs, užtikrinant, kad rezultatai atlaikytų teisinę kontrolę. Taip pat daugiausia dėmesio skiriama būtiniausių reikalavimų ir kontrolės mechanizmų, taikomų dirbtinio intelekto taikymams finansų sektoriuje, kūrimui.	https://www.athene-center.de/en/news/news/ai-against-money-laundering-1554 https://www.sit.fraunhofer.de/de/presse/details/news-article/show/ki-gegen-geldwaesche/
14	Latvija	Algoritmai	Latvijos viešųjų pirkimų stebėsenos biuras integravo "ZoomChart" programinę įrangą, kad galėtų pateikti funkcionalią ir vizualiai patrauklią informaciją apie viešųjų pirkimų veiklą.	https://zoomcharts.wordpress.com/2015/03/09/zoomcharts-on-the-procurement-monitoring-bureau-of-latvia-website/
		DI	Latvijos vyriausybė inicijavo dirbtinio intelekto technologijų integravimą į viešojo administravimo sistemas. Tai apima planus plačiai diegti dirbtinio intelekto sprendimus, skirtus gerinti paslaugų teikimą ir veiklos efektyvumą valstybės ir savivaldybių institucijose.	https://polygant.net/blog/artificial-intelligence-will-become-part-of-the-public-administration-system-in-latvia
		DI	Latvijoje įdiegta elektroninių viešųjų pirkimų sistema, skirta tobulinti viešojo sektoriaus viešuosius pirkimus skatinant atvirą tiekėjų konkurenciją, užtikrinant veiksmingą biudžeto lėšų naudojimą ir mažinant korupcijos riziką. Nors EPS didina skaidrumą, turimoje informacijoje nėra išsamiai aprašytos konkrečios AI funkcijos sistemoje	https://www.liaa.gov.lv/en/article/sorser-a-attracts-eu127-million-ai-driven-tools-supply-chain-and-procurement
15	Lietuva	Algoritmai „Arachne“	Jos pagrindinė funkcija - nustatyti projektus, paramos gavėjus, sutartis ir rangovus, kurie gali būti rizikingi, pavyzdžiui, dėl sukčiavimo, interesų konfliktų ar kitų pažeidimų.	https://nma.lrv.lt/lt/apie-nma/tarptautinis-bendradarbiavimas/kiti-projektai/

		DI „Sakalo akis“	Naudojant pažangių technologinių priemones ir inovatyvių organizacinių sprendimų pagalba užtikrinti efektyvesnį grėsmių nacionaliniam saugumui vertinimą, rizikų prognozavimą ir užkardymą, sunkiausių nusikaltimų atskleidimą ir tyrimą.	https://vrm.lrv.lt/lt/naujienos/sakalo-akis-naujas-analitikos-vystymo-projektas-kovai-su-hibridinemis-gresmemis-ir-organizuotunu-sikalstamumu/
		DI „Viesieji Pirkimai AI“	Sistema automatiškai analizuoja CVP IS duomenis ir identifikuoja aktualius viešuosius pirkimus pagal vartotojo veiklos sritį. Ji leidžia greitai peržiūrėti konkurso sąlygas, pateikiant aiškius paaiškinimus bei svarbiausius akcentus. Naudodama DI, sistema ne tik sumažina rankinio darbo poreikį, bet ir padeda rengti atsakymus į tiekėjų klausimus ar ruošti pasiūlymus, taip ženkliai taupydama laiką bei resursus.	https://viesiejipirkimai.ai/2025/04/17/kas-yra-viesieji-pirkimai-ai-ir-kaip-jis-veikia/
16	Liuksemburgas	DI/ ML „VATCalc“	Priemonė palengvina elektroninę keitimąsi apskaitos duomenimis tarp organizacijų ir mokesčių institucijų, tokiu būdu užtikrinant, jog dokumentai nebus modifikuojami/ manipuliuojami procese.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		Algoritmai „Arachne“	Sukurta duomenų gavybos priemonė, kuri sujungia projektų duomenis su išorės duomenų bazėmis ir naudoja rizikos rodiklius, kad pažymėtų didelės rizikos ES finansuojamas sutartis. Sudaroma galimybė užtikrinti skaidrumą, nes vyriausybės sutarčių duomenys yra prieinami analizei ir viešajai kontrolei. „Arachne“ pagalba nustatomi projektai arba rangovai, kuriems gali kilti sukčiavimo ir (arba) interesų konflikto rizika.	https://employment-social-affairs.ec.europa.eu/policies-and-activities/funding/european-social-fund-plus-esf/what-arachne_en#:~:text=,conflict%20of%20interest%20and%20irregularities
17	Malta	DI	Malta, Jungtinė Karalystė, Kanada, Nyderlandai ir Airija naudoja dirbtinio intelekto sistemą, kuri kasdien lygina viešuosiuose šaltiniuose nurodytą turtą su turtu, deklaruotu PVM ir mokesčių deklaracijose.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		Blokų grandinės technologija	Pagal šį projektą MITA ir Maltos universitetas bendradarbiauja kurdami pirmąjį „išmaniosios sutarties“ prototipą, kad jų viešųjų pirkimų sutartys taptų išmaniosiomis sutartimis. Šiuo būdu viešųjų pirkimų sutartys taptų skaidresnės, kiltų mažesnė rizika manipuliacijai, atsirastų didesnis prieinamumas bei audito galimybės.	Maltos informacinių technologijų agentūra (MITA), Išmaniosios viešosios sutartys

18	Nyderlandai	DI/ MM „SiRi“	2019 m. Nyderlandų mokesčių institucijos, siekdamos nustatyti socialinių išmokų sukčiavimo atvejus, naudojo savarankiškai besimokantį algoritmą, kad sukurtų rizikos profilius. Valdžios institucijos skyrė baudas šeimas vien dėl įtarimų sukčiavimu, pagrįstų sistemos rizikos rodikliais. Didelis kiekis šeimų, dažnai gaunančių mažesnes pajamas arba priklausančių etninėms mažumoms, buvo įstumtos į skurdą dėl pernelyg didelių skolų mokesčių agentūrai.	https://algorithmwatch.org/en/syri-netherlands-algorithm/
		DI „CoPilot“	Nyderlanduose „CoPilot“ naudoja Saugos regionas Zuid-Holland Zuid, kad padėtų darbuotojams rengti tekstus ir apibendrinti dokumentus, taip padidindamas administracinį veiksmingumą.	https://algoritmes.overheid.nl/en/algoritme/microsoft-copilot-safety-region-zuidholland-zuid/77178161
19	Lenkija	DI/ MM	Lenkijos Teleinformatyczny Izby Rozliczeniowej (STIR) sistema, analizuodama bankų ir kredito unijų teikiamus duomenis, kasdien praneša sąskaitų duomenis ir kliringo duomenis apie visas mokesčių mokėtojų atliktas operacijas. Tai leidžia Nacionalinei mokesčių administracijai (NRA) nustatyti galimus sukčiavimus realiuoju laiku.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		DI „ETNA“	ETNA sistema yra skaitmeninė platforma, sukurta Lenkijos centriniame kovos su korupcija biuru (CBA), skirta veiksmingai tvarkyti ir apdoroti pranešimus apie korupciją. Ji supaprastina piliečių pateiktos informacijos apie įtariamą korupciją ar etikos pažeidimus, susijusius su valstybės pareigūnais, priėmimą, kategorizavimą ir pirminį vertinimą.	https://www.epac-eacn.org/news?tx_news_pi1%5Baction%5D=detail&tx_news_pi1%5Bcontroller%5D=News&tx_news_pi1%5Bnews%5D=206&cHash=89a63f9c16113337afa5c004a8f4e8c3&fbclid=IwY2xjawJ2UgJleHRuA2FlbQIxMAABHpOCHpQRO7e6SiM4WPUIcSzPFMrIE5oKLTgIdHB7FsBMwsxmXJ-pnrIBO350_aem_RM0uV_Utq7r7pQ1GnowCFg
		MM „DIGIWHIST“	"OpenTender" platformoje (ES DIGIWHIST projektas) kaupiami Lenkijos viešųjų pirkimų duomenys ir skaičiuojami skaidrumo rodikliai (pvz., "gerų pirkimų" balai). Ji taiko „raudonos vėliavos“ rodiklius, kad nustatytų įtartinus konkursus. Duomenys susiejami su informacija apie įmones, kad išryškėtų neįprasti modeliai (pvz., maža konkurencija, pasikartojantys laimėtojai).	https://projects.research-and-innovation.ec.europa.eu/en/projects/success-stories/all/new-online-tools-shine-light-public-spending

20	Portugalija	DI/ MM „VATCalc“	Priemonė palengvina elektroninį keitimąsi apskaitos duomenimis tarp organizacijų ir mokesčių institucijų, tokiu būdu užtikrinant, jog dokumentai nebus modifikuojami/ manipuluojami procese.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		Blokų grandinės technologija	Projektais siekiama modernizuoti viešuosius pirkimus. Darbuotojai daug laiko praleidžia atlikdami pasikartojančias rankines užduotis, dėl kurių kyla didelė žmogiškųjų klaidų rizika. Sistema apima procesų automatizavimą, prašymų tvirtinimą, dokumentų rengimą ir tiekėjų tvirtinimą. Naudojant blokų grandinę, projektu siekiama užtikrinti didesnę viešųjų pirkimų saugumą ir padidinti informacijos atsekamumą.	https://ec.europa.eu/assets/grow/growth/_toolbox/pp-emerging-tech/tabledet.html?d=15
21	Prancūzija	DI	Prancūzija naudoja dirbtinio intelekto palydovinių vaizdų skenavimą, kad nustatytų akivaizdžiai matomo vartojimo požymius. Tai gali būti keli automobiliai, baseinai ir pan. kurie nesuderinami su asmens gaunamomis pajamomis. Naudinga nustatant nekilnojamojo turto mokesčius.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		MM/ DI	Nevyriausybinių organizacijų "Anticor" kuria DI/MM modelį, skirtą analizuoti viešųjų pirkimų sutarčių sudarymo tvarką, kad būtų galima nustatyti pažeidimus. Sistema lygina tikėtiną ir faktinę konkurso dalyvių elgseną, kad pažymėtų sutartis, kuriose yra didelė korupcijos tikimybė (nereikalaujant žmogiškųjų resursų). Kova su pasiūlymų klastojimu ir favoritizmu - priemone siekiama automatiškai nustatyti korupcinius viešųjų pirkimų sandorius (pvz., suklasotus pasiūlymus, interesų konfliktus) ir netgi kiekybiškai įvertinti "tikrąjį pažeidimų kiekį" viešųjų pirkimų srityje.	https://www.lemoniteur.fr/article/marches-publics-anticor-s-arme-de-l-intelligence-artificielle-pour-detecter-les-anomalies.2336115 https://instituteuropa.eu/fr/nos-articles/ia-et-marches-publics-vers-plus-de-transparence
		DI „CFVR“	Ūkio ministerijos mokesčių departamentas (DGFIP) naudoja dirbtinio intelekto valdomą sistemą CFVR ("Ciblage de la Fraude et Valorisation des Requêtes"). Ji naudoja DI kad automatiškai pastebėtų anomalijas ar modelius, atitinkančius PVM vengimo, nedeklaruotų pajamų ar kitokio sukčiavimo požymius. Kova su finansine korupcija ir sukčiavimu - mokesčių vengimo schemas ir sukčiavimo atvejus nustato daug greičiau nei tradiciniai auditai. Tai pagerina viešųjų finansų vientisumą ir atgraso nuo korupcijos, nes padidėja tikimybė ją aptikti (2024 m. maždaug pusė visų įmonių mokesčių auditų buvo inicijuoti dėl šio DI rezultatų).	https://www.economie.gouv.fr/actualites/detection-des-fraudes-analyse-de-donnees-comment-lia-fait-son-entree-bercy

22	Rumunija	DI/ MM	Rumunija teigia, kad per pastaruosius 12 mėnesių dėl dirbtinio intelekto ir robotų diegimo iki 1 proc. padidino PVM įplaukas.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		DI/ MM	AADR (Rumunijos nacionalinė skaitmeninės darbotvarkės agentūra) kuria pokalbių robotą, kuris padės orientuotis viešųjų pirkimų procesuose.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en
23	Slovakija	-	-	-
24	Slovėnija	Algoritmai „SKRINJA“	Pagrindinė jos funkcija - suteikti valdžios institucijoms saugią, BDAR reikalavimus atitinkančią platformą struktūrizuotiems duomenims analizuoti, taip didinant viešojo administravimo skaidrumą, efektyvumą ir strateginį planavimą.	https://oecd-opsi.org/innovations/skrinja-chest-using-emerging-technologies-for-better-digital-public-services-and-data-driven-decision-making-in-slovenia/
		Algoritmai	Žmogiškųjų išteklių, finansų ir viešųjų pirkimų duomenys buvo sujungti su išorės duomenų šaltiniais. Analizės rezultatai parodė, kad esama didelių galimybių sumažinti su viešaisiais pirkimais susijusias išlaidas.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en
25	Suomija	DI/ MM	Suomijos valstybės išdas planuoja automatizuoti e. sąskaitų tvarkymą pasitelkdamas dirbtinį intelektą. Manoma, kad dirbtinio intelekto įrankiai galėtų per kelias sekundes išanalizuoti sąskaitą faktūrą ir rasti reikiamą informaciją, pavyzdžiui, sutarties numerį ir sumą.	https://ec.europa.eu/digital-building-blocks/sites/display/DIGITAL/eInvoicing+in+Finland
		MM „Hansel Oy“	Sistema skirta, kad būtų užtikrintas išlaidų skaidrumas po viešųjų pirkimų konkurso laimėjimo. Hansel Oy išbandė mašininio mokymosi sprendimą, skirtą duomenims kategorizuoti pagal Jungtinių Tautų standartinį produktų ir paslaugų kodą (UNSPSC).	https://tutkihankintoja.fi/?lang=en

		Algoritmai	Šiuo metu veikia 26 robotai, automatizuojantys 70 procesų. Automatizuoti procesai apima pirkimo sąskaitų faktūrų tvarkymą ir tiekėjų registro tvarkymą. Bendrovė „Palkeet“ nustato ir įvertina automatizuotinus procesus, o automatizavimo ekspertai bendradarbiauja su paslaugų savininkais, kad sukurtų ir įdiegtų robotus.	https://interoperable-europe.ec.europa.eu/sites/default/files/news/2020-06/D.01.06_Final_report_v3.00.pdf
26	Švedija	DI/ MM	Švedija naudoja dirbtinį intelektą, kad nustatytų ir išryškintų mokesčių rizikos problemas, kai įmonės kreipiasi dėl naujų įmonių steigimo. Sistema gali peržiūrėti, ar registracijos paraiškose nėra mokesčių vengimo požymių, taip pat ji padėjo pagreitinti paraiškų teikimo procesą.	https://www.vatcalc.com/artificial-intelligence/tax-authorities-adopt-ai-for-tax-fraud-and-efficiencies/
		DI/ MM	Į e. pirkimų platformą integruojamas dirbtinio intelekto asistentas. Šis įrankis gali atlikti reikalavimų ir kito pirkimo medžiagoje esančio teksto semantikos patikrą, kuri sumažins riziką, kad dalyviai neteisingai supras pirkimo medžiagą, taigi sumažins ir dalyvio riziką.	https://www.reusecompany.com/events/public-procurement-conference-2020
		Blokų grandinės technologija	Sistemos pagalba nekilnojamojo turto pardavimai buvo registruojami privačioje blokų grandinėje, taip sukuriant nuolatinę, nuo klastojimo apsaugotą sandorių proceso knygą. Visos šalys (pirkėjai, pardavėjai, bankai, brokeriai, vyriausybė) galėjo stebėti sandorio statusą realiuoju laiku, naudodamos kriptografinę patikrą. Saugūs nekilnojamojo turto sandoriais siekiama užkirsti kelią sukčiavimui žemės nuosavybės teisės srityje ir užtikrinti nekilnojamojo turto sandorių skaidrumą. Turint nekeičiamą įrašą, kas ir kada su kuo sutiko, tampa neįmanoma slapta pakeisti sutarčių ar nuosavybės įrašų. Be to, automatizavus tikrinimo veiksmus, pagreitėja pardavimo sandorio užbaigimo procesas (kuris tradiciškai gali užtrukti kelis mėnesius).	https://www.reuters.com/article/technology/sweden-tests-blockchain-technology-for-land-registry-idUSKCN0Z30DC/
27	Vengrija	Blokų grandinės technologija	Sistema skirta konkurso dokumentams šifruoti kaip trečiosios šalies žiniatinklio paslauga su alternatyvia darbalaukio programa. Subjektai gali šifruoti savo konkurso dokumentus ir siųsti arba įkelti užrakintą pasiūlymą nustatytu atskiru kanalu. Turėdamos neiššifruotą raktą perkančiosios organizacijos gali atrakinti - taigi atverti - konkurso dokumentus. Per laiką, praėjusį tarp pasiūlymų užrakinimo ir atrakinimo, raktas neegzistuoja, todėl matematiškai neįmanoma prieiti prie konkurso dokumentų.	https://single-market-economy.ec.europa.eu/single-market/public-procurement/digital-procurement/emerging-technologies-public-procurement_en

		Algoritmai "Red Flags"	„Raudonos vėliavos“ (ang. „Red Flags“) - tai atvirojo kodo internetinė priemonė (ją sukūrė „Transparency International HU“, „K-Monitor“ ir kt.), kuri kasdien automatiškai tikrina skelbimus apie viešuosius pirkimus iš „EU Tenders Electronic Daily“ ir Vengrijos duomenų bazių. Kiekvienam skelbimui apie viešąjį pirkimą sistema naudodama specialų algoritmą, taiko ~40 rodiklių rinkinį (pvz.: vieno pasiūlymo sutartis, skuboti terminai, laimėtojo ryšiai su pareigūnais). Tada ši priemonė išryškina (viešai skelbiamoje švieslentėje) tuos konkursus, kuriems būdingi keli įspėjamieji požymiai. Sistema prižiūrima ir prireikus atnaujinama, įtraukiant naujus rodiklius (Ją įkvėpė „Arachne“, tačiau „Red Flags“ yra atvira visiems.	https://antifraud-knowledge-centre.ec.europa.eu/document/download/935370f5-b1a0-41b1-9bc9-026977497a20_ga#:~:text=The%20Red%20Flags%20tool%20was,the%20fight%20against%20corrupt%20procurements
--	--	---------------------------	---	--