Vilniaus universiteto
Filosofijos fakulteto
Bakalauro studijų programa „Kriminologija“

Vaiva Žiogaitė

Kriminologijos studijų programa
Bakalauro darbas

Dirbtinio intelekto taikymas teisėsaugoje: technologiškai pažengusių šalių atvejų analizė

Darbo vadovė: Asist. Dr. Maryja Šupa

Vilnius
2023

Turinys

Santrauka

Dirbtinis intelektas susilaukia vis daugiau dėmesio kuo įvairesnėse srityse, taip pat ir teisėsaugoje. Pasitelkiant DI technologijas teisėsaugos sistemoje galima sutaupyti lėšų ir palengvinti bei pagreitinti kasdienius policijos veiklos procesus. Tyrimų šia tematika Lietuvoje trūksta, tačiau galime paminėti Dr. D. Barysės atliekamus tyrimus, kurie remiasi į technologijų taikymą teisminiame procese. Atsižvelgiant į tai, iš viešai prieinamos informacijos, siekta išsiaiškinti, Estijos, Jungtinės Karalystės, Belgijos, Prancūzijos bei Vokietijos patirtį bei požiūrį diegiant ir taikant DI technologijas teisėsaugos sistemoje. Iš surinktų duomenų galime teigti jog šalys nėra linkusios pakankamai detaliai ir plačiai aprašyti DI technologijų grėsmių bei naudų, o tai gali iškreipti visuomenės matomą DI vaizdą. Visos tiriamos šalys nurodo saugumo, patikimumo, skaidrumo, duomenų apsaugos, nediskriminavimo aspektus, o tai iš esmės principai, kurie saugo jautriausias visuomenei temas. Šalys išsiskiria pavieniais principais, kurie nesusilaukia didelio dėmesio visuomenėje, tačiau mokslinėje literatūroje šie principai yra itin svarbūs visame technologijų gyvavimo cikle. DI naudojimo dėsningumas matosi ties vagysčių-įsilaužimų prognozės bei duomenų-dokumentų analizės technologijomis. Didžioji dauguma tyrime nurodomų technologijų orientuotos į duomenų analizę ir tik mažoji dalis į fizinę kontrolę (pvz.: vaizdo stebėjimo priemones), tai suponuoja jog naudojamos sistemos yra gan mažos rizikos, o tinkamas jų pritaikymas gali ženkliai pagerinti teisėsaugos našumą.

Summary

Artificial intelligence is becoming increasingly important in a variety of fields, including law enforcement. The use of AI technologies in law enforcement can save money and make everyday police processes easier and faster. There is a dearth of research on this topic in Lithuania, but mention can be made of Dr Barysė's research, which is based on the application of technology in the justice sector. The aim of this study was to identify the experiences and approaches of Estonia, the United Kingdom, Belgium, France and Germany in the introduction and application of AI technologies in law enforcement based on publicly available information. From the data collected, it can be concluded that countries lack detailed and comprehensive descriptions of the threats and benefits of AI technologies, which may distort public perceptions of AI. All countries surveyed refer to security, reliability, transparency, privacy and non-discrimination, essentially principles that protect the most sensitive issues for society. Countries stand out with individual principles that usually do not receive much

public attention, but in the academic literature, these principles are crucial for the entire life cycle of the technology. The pattern of AI used can be seen in technologies for intrusion prediction and data or document analysis. The vast majority of technologies identified in the study focus on data analysis and only a minority on physical control (e.g. surveillance tools), suggesting that the systems used are relatively low-risk and that their proper application can significantly improve law enforcement performance.

Įvadas

Dirbtinis intelektas (DI), dėl savo teikiamos naudos vis dažniau susilaukia dėmesio kuo įvairesnėse srityse. Dabartinėmis sąlygomis, kai nusikaltimai įgauna vis naujas formas, o teisėsaugos biudžetai yra pakankamai limituoti, iškyla poreikis, kuo efektyviau panaudoti policijos išteklius nusikaltimams užkardyti ir išaiškinti (Casey, Burrell ir Sumner, 2019, p. 104). Būtent DI paremtomis programomis, teisėsaugos sistemoje galima sutaupyti lėšų (Boahemaa, 2019, p. 1), palengvinti bei pagreitinti kasdienius policijos veiklos procesus (Meijer ir Wessels, 2019, p. 1031 – 1133; Casey, Burrell ir Sumner, 2019, p. 104; Ibarra, Douglas ir Tharmarajah, 2020, p. 23). Tačiau jei sistemos bus netinkamai sukurtos ir naudojamos, DI teisėsaugos sistemoje gali sukelti žalos. Pasireikšti gali programų šališkumas, diskriminacija (Moses ir Chan, 2018, p. 810; Joh, 2018, p. 1142; Sharma et. al., 2019, p. 8; Ibarra, Douglas ir Tharmarajah, 2020, p. 11). Rizika gali kilti duomenų apsaugai (Wirtz, Weyerer ir Geyer, 2019, p. 603; Degeling ir Berendt, 2018, p. 355), o nutekintais duomenimis gali pasinaudoti įvairūs asmenys siekiantys pakenkti – konkrečiam asmeniui, asmenų grupei ar valstybei. Norint jog sistemos būtų kuriamos bei diegiamos tinkamai, tam reikalingi bendri tarptautiniai DI etikos principai, kuriuos pirmieji išleido UNESCO. Jose pažymima duomenų apsaugos, nešališkumo, tvarumo svarba, bei tokie aspektai, kaip bendradarbiavimas tarp valstybių dalinantis DI nauda (UNESCO, 2021, p. 20 – 23).

Lietuvoje DI taikymo teisėsaugoje tema yra pakankamai nauja, todėl šis darbas tampa svarbus dėl tyrimų trūkumo. Galime paminėti Dr. D. Barysės atliekamus tyrimus (D. Barysė, 2021; D. Barysė ir R. Sarel, 2022), kurie remiasi į technologijų taikymą teisminiame procese. Tuo tarpu užsienio literatūroje ši tema sulaukia daugiau dėmesio ir yra nagrinėjama aktyviau, tačiau globaliu mastu skirtingų šalių palyginimų, šioje srityje nėra daug. Šis darbas suteiks informacijos pagrindą apie DI taikymo teisėsaugoje padėtį kitose šalyse, pritrauks dėmesį ir duos pagrindą tęsti tyrinėjimus šiame lauke.

Šio darbo tikslas – palyginti technologiškai pažangių šalių viešai prieinamą informaciją apie DI taikymą bei naudojimą teisėsaugoje.

Darbo uždaviniai:

1. Paanalizuoti DI sampratą, DI etikos principus ir aptarti DI technologijų galimas rizikas bei naudas.
2. Palyginti tiriamų šalių DI strategijas (DI etikos principai, galima nauda bei žala, į žmogų orientuoto DI kryptis)

3. Nustatyti, kaip yra užtikrinamas sistemų saugumas bei kokius duomenų apsaugos įstatymus šalys nurodo DI kontekste.

4. Aprašyti bei palyginti tiriamų šalių DI naudojimą teisėsaugoje.

Tyrimo metodas: Uždaviniams atskleisti bus analizuojami duomenys taikant keletos atvejų analizės metodą (angl. *Multiple-case study*), kuris leis iš didelio medžiagos kiekio išanalizuoti ir tarpusavyje palyginti temai aktualius aspektus: DI principus, rizikas, naudas, įstatymus, bei atrasti dėsningumus ir skirtumus tarp viešai randamų pavyzdžių, kur teisėsaugoje naudojamas DI. Siekiant užtikrinti duomenų patikimumą, pasitelkiama įvairaus tipo medžiaga: tarptautinių organizacijų dokumentai, mokslinė literatūra, nacionaliniai šalių dokumentai, teisės aktai bei DI organizacijų publikacijos, kurios vėliau pagal uždavinio tikslą sugretinamos, palyginamos ir apibendrinamos. Technologiškai pažengusios šalys (TPŠ) – tai šalys, kurios skaitomoje literatūroje pasižymėjo dideliu dėmesiu inovacijoms bei šalies vystymuisi naudojant DI. Teorinėje dalyje aptariami DI etikos principai, jo rizikos ir naudos bei į žmogų orientuoto DI svarba – jiems atskleisti analizuojama mokslinė literatūra bei tarptautinių organizacijų rekomendacijos. Šios analizuojamos koncepcijos papildys tyrime gaunamą informaciją. Tokia darbo struktūra suteiks abipusį požiūrį – iš mokslinės bei viešoje erdvėje esančios informacijos pusės. Tai suteiks įžvalgų, kiek šalys, viešai prieinamuose šaltiniuose, atspindi mokslinėje literatūroje akcentuojamų aspektų.

Šiame tyrime buvo taikoma tikslinė atranka, kaip TPŠ, buvo pasirinktos: Jungtinės karalystės (JK), Belgija, Vokietija, Prancūzija bei Estija. Pasirinkimą lėmė didelis šalių dėmesys inovacijų plėtrai teisėsaugos sistemoje, dažnas pasikartojimas analizuojamoje literatūroje (*žiūrėti 1 priedą*), bei jų geografinė padėties įvairovė, kuri suteiks bendresnę bei aktualesnę informaciją apie požiūrį į DI, jo taikymą ir naudojimą Europos geografinėje zonoje. Pasirinktų šalių kiekis suteiks galimybę daryti apibendrinančias išvadas, kurios kaip gerųjų praktikų pavyzdžiai, būtų naudingos šalims norinčioms siekti inovacijų teisėsaugoje.

Darbo struktūrą sudaro: *teorinė medžiaga* – kurioje aptariami DI principai, šių technologijų galima žala bei nauda teisėsaugoje, padės įžvalgomis papildyti tiriamąją dalį; *tyrimas* – kuriame atsakoma į darbo klausimus; *rezultatų apibendrinimas ir diskusija* – joje išdėstomos viso darbo įžvalgos bei galutinės *išvados*.

1. Dirbtinio intelekto apibrėžimas, principai, nurodoma rizika ir nauda mokslinėje literatūroje

1.1. Dirbtinio intelekto apibrėžimo problemos

Visuomenėje DI naudojamas apimti labai platų technologijų spektrą, todėl pačioje literatūroje linkstama prie labiau specifiško – mašininio mokymosi (MM)(ang. *Machine learning*) ar gilaus mokymosi (GM)(ang. *Deep learning*) priemonių pavadinimų. Paprasčiausiu būdu DI yra paaiškinamas „<...> kaip technologijų rinkinys, kuris apima duomenis, algoritmus ir apdorojimo galią <...>“ (Europos taryba, 2020, p. 2) tačiau būtent toks apibrėžimas yra ganėtinai abstraktus ir suteikia mažai informacijos, kas iš esmės yra pastebima ir daugelyje kitų mokslinėje literatūroje naudojamų apibrėžimų. Šiame skyriuje yra svarbu išskirti bei atskirti sistemų kategorijas, kurios minimos aprašant kuriamas ar veikiančias priemones, tai: DI, MM, bei GM priemonės. Kadangi mokslinėje literatūroje neretai yra diskutuojama dėl prasto (DI) termino bei jam keliamų abejonių (Babuta ir Oswald, 2019, p. 4; Europos taryba, 2018, p. 30) šioje dalyje taip pat bus siekiama labiau atskleisti DI ir jo porūšių apibrėžimo sunkumus, bei paanalizuoti literatūroje pateiktas sampratas.

Užsienio mokslinėje literatūroje naudojami apibrėžimai kaip „silpnas“/ „stiprus“ DI (ang. *Weak/ Strong AI*), lietuviškuose straipsniuose verčiami, kaip tam tikros srities bei visuotinis DI. Tam tikros srities bei „silpnas“ DI gali efektyviai nustatyti dėsningumus, mokytis iš didelių duomenų kiekių ir ganėtinai tiksliai prognozuoti (Europos taryba, 2018, p. 30), tačiau tai vyksta tik konkrečios srities ribose (pvz.: teisinių dokumentų analizė) todėl ir jo nauda yra ribota (Amilevičius, 2017, p. 22). Tuo tarpu visuotinis DI gali pats mokytis, suvokti ir kurti naujas žinias (Europos taryba, 2018, p. 30; Amilevičius, 2017, p. 23). Pastarosios sistemos, dėl savo sudėtingumo, kol kas neegzistuoja ir lieka vien fikcinėmis.

2019 metų Lietuvos dirbtinio intelekto strategijoje yra remiamasi Europos tarybos apibrėžimu, kad DI – tai „<...> sistemos, kurios demonstruoja protingą ir sumanų elgesį, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti“ (Europos taryba, 2018, p. 1). Pagal D. Amiliavičių, kuris yra vienas iš specialistų dirbusių prie Lietuvos DI strategijos, dirbtinis intelektas „yra specifinių, sparčiai besivystančių technologijų grupė, kurių funkcionalumų rezultatai siauroje taikymo srityje prilygsta žmogaus lygiui, o kartais jį jau ir pranoksta“ (Utka, 2022, p. 122). Labai panaši mintis buvo išreikšta ir UNICRI ir INTERPOL išleistoje, DI skirto teisėsaugai,

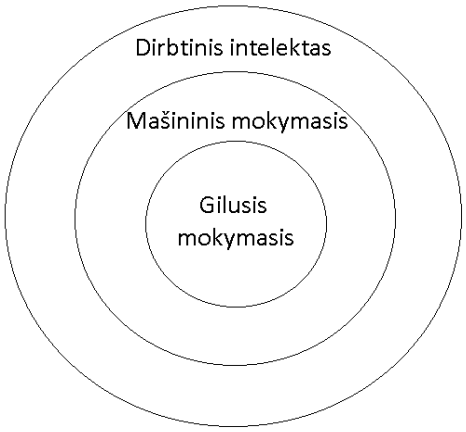
ataskaitoje, jog DI naudojasi panašiais į žmogaus intelektą procesais: balso atpažinimas, kalbos vertimas, sprendimų priėmimas, problemų sprendimas ir to gali mokytis iš duomenų bazėse esančių dėsningumų, nereikalaujant aiškių nurodymų iš žmogaus (UNICRI ir INTERPOL, 2020, p. 51).

Tačiau Saulius Keturakis pažymi jog DI negali sukurti kažko visiškai naujo, DI užsiima tik subtiliu duomenų perkomponavimu (Utka, 2021, p. 123), šiai nuomonei pritaria ir Murauskas atskleisdamas jog šios sistemos iš esmės padeda išanalizuoti kompleksinę informaciją, gali padėti ją struktūrizuoti bei suteikti išvadas (Murauskas, 2020, p. 56). Visi šie apibrėžimai skirti apibūdinti tai pačiai sistemai – DI, tačiau turi skirtingą konotaciją. Viena pusė teigia jog tai sistema, kuri gali pralygti žmogaus intelektui ir veikti „gana“ (žodžio pasirinkimas labai atsargus, bei tiksliai neapibrėžia kiek sistema yra savarankiška daryti sprendimus) savarankiškai, o antra pusė prilygina DI sistemas iki paprastų pagalbinių technologijų žmogaus kasdienei veiklai. Kadangi DI apima ir MM bei GM sistemas, kurios savo struktūra skiriasi ne tik tarp savęs, bet ir nuo bendrojo DI, jos sumaišomos į vieną DI terminą ir sukelia daug sunkumų literatūroje.

MM priemonių apibūdinimų, mokslinėje literatūroje galime rasti tokių kaip: „Paprastai MM algoritmai veikia mokydamiesi iš istorinių duomenų ir apibendrindami juos dar nematytiems duomenims” (Suresh ir Guttag, 2021, p. 1) arba „ <...> 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). Aprašoma ir tai, kad MM sistemos gali klasifikuoti duomenis remiantis stambiais apibendrinimais, kai didesnis detalumas leistų pasiekti geresnių rezultatų (Moses ir Chan, 2018, p. 811). Tokiu pavyzdžiu algoritmas gali generalizuoti pavojingą vairavimą pagal bendrą požymį „jaunas ir vyras“, nors kintamasis „agresyvus“ būtų daug efektyvesnis, tai tam tikra prasme parodo ir sistemos ribas– apie kurias kalbėjo ir anksčiau minėtas Amiliavičius. Mokslinėje literatūroje aprašant terminus neretai buvo pastebima jog autoriai naudoja internetiniuose žodynuose esančius apibūdinimus, kas iš dalies atskleidžia susidariusį nenuoseklumą DI apibrėžimo kontekste. A. Lyuben su kolegomis (Lyuben et. al., 2021, p. 26) savo darbe naudojo štai tokį žodyne (www.dictionary.com) rastą apibrėžimą – „Kompiuterio gebėjimas apdoroti ir įvertinti duomenis ne tik pagal užprogramuotus algoritmus, bet ir pagal kontekstą“ . O Europos taryba, aprašydama MM priemones pamini jog tai kompiuterių mokslo dalis, kurioje programinės įrangos mokosi iš patirties (Europos taryba, 2018, p. 33). Galime pastebėti, kad MM apibrėžimuose nebėra matyti žmogui prilystančio arba pernokstančio intelekto galimybių.

GM sistemos kol kas mažiausiai nagrinėjamoje literatūroje aptiktas terminas, tačiau taip pat yra DI dalis, o dar tiksliau – MM pogrupis (Jakhar ir Kaur, 2019, p. 1). GM naudoja daugiasluoksnius „gilus“ neuroninius tinklus, kurie gali rasti sudėtingus modelius dideliuose duomenų rinkiniuose, tai „Toli gražu ne dirbtinė nuojauta, sąmonė ar visuotinis intelektas <...>“ (Asaro, 2019, p. 42). Sistema vadinama „gilusis“ mokymasis, kadangi joje veikia „algoritmai, imituojantys smegenų biologinių neuroninių tinklų architektūrą“ (Jakhar ir Kaur, 2019, p. 1). Būtent ši sistema turi ryškiausią išskirtinumą, dėl kurio yra ganėtinai sudėtinga ją sumaišyti su kitomis minėtomis sistemomis. GM ypatumas yra tai jog jis gali atlikti ne tik visas MM funkcijas bet ir apdoroti itin didelius duomenų kiekius bei užtikrinti sprendimo priėmimo galimybes pvz.: MM gali užtikrinti vaizdų aptikimą savaeigiams automobiliams, o GM gali priimti sprendimus, kuria kryptimi jiems važiuoti, kad išvengti kliūties (Sultan et. al., 2020, p. 5).

Norint vaizdžiai suvokti, kokiose lygmenyse yra visos trys aptartos sistemos padeda vizualinė priemonė *1 pav*.



1 pav. Jakhar, D. Kaur, I. „ Artificial intelligence, machine learning and deep learning: definitions and differences” 2019

Iš esmės mokslinėje ir tarptautinių organizacijų literatūroje, negalima pastebėti nuoseklumo DI sistemų apibrėžime. Tačiau kai kur išlieka pasikartojanti savybė – žmogaus intelekto bruožų ir galimybių mimikavimas, o tai neturi ryškaus atotrūkio nuo populiariajame diskurse esančio suvokimo. Taip pat DI apima tiek MM tiek GM sistemas, todėl šis faktas gali turėti įtakos ganėtinai sunkiai atskiriamai terminijai. MM tai DI dalis, kuri panaudoja algoritmus dėsningumų aptikimui jau esamuose duomenyse ir išsimokina save numatyti naujus duomenis (Sultan et. al., 2020, p. 4). GM, kaip ir minėta anksčiau yra MM pogrupis, kuris savo funkcionalumu yra daug sudėtingesnis ir galintis valdyti labai didelį duomenų kiekį (Sultan et. al., 2020, p. 4; Europos komisija, 2020, p. 5; Asaro, 2019, p. 42).

Apibendrinant galime matyti jog mokslinėje literatūroje daugiausia diskusijų kyla dėl DI bei MM priemonių apibrėžimų atskirties. Paskutiniąja pastraipa siekta nustatyti šią atskirtį tarp visų sistemų (DI, MM, GM), išskiriant ryškiausius jas apibūdinančius literatūroje rastus bruožus. Svarbu pabrėžti jog siekiant išlaikyti autorių autentiškumą, šiame darbe cituojant TPŠ naudojamas DI priemones, bus

naudojamas toks terminas, kuris nurodytas literatūroje. Rašant bendrai daugiausia bus naudojamas DI terminas, norint tikslumo – MM arba GM.

1.2. Etikos principai skirti dirbtinio intelekto technologijoms

Šiame darbe yra svarbu atskleisti tai kokie DI principai ir etikos taisyklės yra akcentuojamos ne tik mokslinėje literatūroje, bet ir tarptautinių organizacijų rėmuose. Kadangi DI sistemos yra ganėtinai nauja tema, principų jai sukūrimas bei įgyvendinimas gali užtikrinti saugumą bei jų naudą 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.

Lyuben su kolegomis nurodo jog teisėsauga turi užtikrinti, kad DI sistemos bei jų veikimas atitiktų „teisingumo, atskaitomybės, skaidrumo ir paaiškinamumo“ (Lyuben et. al., 2021, p. 23) reikalavimus, kurie nurodyti, kaip kertiniai DI principai. UNESCO – tai Jungtinių Tautų švietimo, mokslo ir kultūros organizacija, kurioje yra daugiau negu 200 valstybių. Ši organizacija remia projektus bei teikia rekomendacijas (švietimo, mokslo, kultūros, įskaitant ir technologijų srityse), o 2021 m. lapkritį priėmė pirmąsias tarptautines DI etikos standartų rekomendacijas, bei savo tinklapyje pristatė jog „Šiame dokumente apibrėžiamos vertybės, principai ir politikos priemonės, kuriomis šalys galės vadovautis kurdamos teisines sistemas, užtikrinančias, kad DI būtų naudojamas, kaip bendram labui skirta jėga“(UNESCO, 2021).

Pirmasis UNESCO nurodomas principas yra – *proporcingumo ir žalos vengimo*. Šioje dalyje apibrėžiamas DI naudojimo pagrindimas: proporcingas tikslui pasiekti; neturi piktnaudžiauti ar pažeisti žmogaus teisių bei šiose UNESCO rekomendacijose užfiksuotų vertybių; DI metodas turi būti pagrįstas moksliškai atsižvelgiant į aplinkybes. Pažymima, kad „DI sistemos neturėtų būti naudojamos socialinio vertinimo ar masinio stebėjimo tikslais“ (p. 20), tai tampa iš esmės svarbiu teiginiu, atsižvelgiant į asmenų privatumą. Žalos vengimo principas literatūroje pateikiamas, kaip siekis kurti rizikų valdymo strategijas bei yra siejamas su saugumu ir manymu jog DI niekada neturėtų sukelti numatytos ar netyčinės žalos (Jobin, Ienca ir Vayena, 2019, p. 9).

UNESCO *Saugumo ir apsaugos* principu nurodo jog saugų ir patikimą DI turėsime tada, kai turėsime tvarias bei privatumą saugančias prieigas prie duomenų bazių, taip kad DI sistemos galėtų mokytis iš kokybiškesnių duomenų. Nurodomas ir poreikis per visą DI sistemos gyvavimo ciklą vengti galimų pavojų bei išpuolių dėl galimo sistemos pažeidžiamumo (UNESCO, 2021, p. 20). Ibarra su kolegomis papildo jog „DI sistemos turėtų gerbti ir išlaikyti privatumo teises ir duomenų apsaugą bei

užtikrinti duomenų saugumą“ (Ibarra, Douglas ir Tharmarajah, 2020, p. 9). Europos veiksmingo teisingumo komisija (CEPEJ, 2018) saugumo principą prijungė prie kokybės, bei jame dėstė, jog MM modelių kūrėjai tūrėtų gebėti pasinaudoti teisėsaugos institucijose esančių specialistų (teisėjų, prokurorų...) bei mokslininkų, iš teisės ir socialinių mokslų, žiniomis (ekonomistai, filosofai...). Tai kūrėjams suteiktų platesnį suvokimą, kaip pritaikyti sistemą tam tikrai sričiai, kaip turėtų vykti komunikaciją apie sistemų naudojimą viešajame sektoriuje, kokie aspektai gąsdintų visuomenę ir t.t.

UNESCO pažymi jog DI subjektai turėtų kuo labiau sumažinti diskriminacinių ar šališkų sistemų rezultatų atsiradimą bei užtikrinti sąžiningumą pagal tarptautinę teisę. Prie *Sąžiningumo ir nediskriminavimo principo* iškyla svarbus aspektas – tai jog valstybė turi stengtis mažinti skaitmeninį atotrūkį ir užtikrinti technologijų naudos pasiekiamumą, o technologiškai pažengusios šalys turi solidarizuotis su mažiau pažengusiomis ir dalytis technologijų teikiama nauda (UNESCO, 2021, p. 20-21). Mokslinėje literatūroje galime surasti ir tokių siūlymų, kaip – duomenų rinkiniams taikyti intersekcionalumo koncepciją, taip siekiant sumažinti šališkumą lyties, rasės bei kitų jautrių temų pagrindu (Berryhill et .al., 2019, p. 69). Intersekcionalumas skirtas aptarti ne tik individualios tapatybės atstovavimą, jis nagrinėja ir kritikuoja galios sistemas, bei kaip šios sistemos kuria nelygybę tam tikrų grupių ir individų atžvilgiu. Žvelgiant į DI kūrimą ir diegimą per intersekcinę prizmę, galima iššifruoti grupės ar individo galią sukuriančias struktūras bei jas pertvarkyti (Ciston, 2019, p. 4).

Tvarumo principu akcentuojama jog DI tvarumo siekimas priklauso nuo jo taikymo skirtingo išsivystymo šalyse ir būtent todėl iškyla nuolatinis DI tvarumo vertinimo poreikis (UNESCO, 2021, p. 21). OECD 2019 m. išleido DI principus, kuriuose nurodė, kad šios sistemos turi teikti naudą žmonijai ir žemei ir suteikti tvaraus vystymosi ir gerovės galimybes. DI priemonės gali užtikrinti tvarumą nuo sunaudojamo popieriaus kiekio mažinimo teisėsaugos kasdienėse veiklose iki elektros vartojimo optimizavimo taip sumažinant tarifus. Papildant, tvarumas kuriant ir diegiant DI sistemas reikalauja ne tik aplinkosaugos, bet ir teisingesnės, lygesnės visuomenės kūrimo, ir taikos skatinimo (Jobin, Ienca ir Vayena, 2019, p. 12).

Teisės į privatumą ir duomenų apsaugą principe pažymima jog darbas su duomenimis bei pati duomenų apsaugos sistema turi vadovautis tarptautinę teisę, vertybėmis bei principais išdėstytais šiose (UNESCO) rekomendacijose. Literatūroje taip pat kyla daug klausimų, kam tenka atsakomybė už DI sistemų veikimą, ir nors UNESCO rekomendacijose ši mintis yra nurodyta prie privatumo ir duomenų apsaugos, autoriai atsakomybę priskiria tiems DI subjektams, kurie projektavo bei diegė tam tikrą programą. Dažnu atveju mokslinėje literatūroje privatumas siejamas su duomenų apsauga,

pasitikėjimu, bei laisve (Jobin, Ienca ir Vayena, 2019, p. 10) taip pat sieja su pagarba duomenų apsaugai ir asmeniniams duomenims (Berryhill et. al., 2019, p. 105; Ibarra, Douglas ir Tharmarajah, 2020, p. 9).

UNESCO įvardijo jog *Žmogiškosios priežiūros bei sprendimo* principas turėtų užtikrinti jog, bet kokioje sistemos stadijoje būtų galimybė priskirti teisinę ar etinę atsakomybę, tiek sistemos, tiek žmogaus klaidos atveju. Galima papildyti jog sistemų kūrėjai turėtų būti indentifikuojami, o DI sistemos – stebimos žmonių (Ibarra, Douglas ir Tharmarajah, 2020, p. 9). Yra nurodoma jog „dirbtinio intelekto sistema niekada negali pakeisti galutinės žmogaus atsakomybės ir atskaitomybės“ (UNESCO, 2021, p. 22) tai gana tiesiogiai sutampa su teisės į privatumą ir duomenų apsaugos principe nurodytų požiūriu.

Bene daugiausiai aprašytas UNESCO principas – s*kaidrumas ir aiškumas*, kurio užtikrinimas tiesiogiai lemia pagarbą žmogaus teisėms ir jo laisvėms. Skaidrumo trūkumas gali lemti iškilusius sunkumus norint teisiškai užginčyti DI sprendimus, bei taip pažeisti teisę į teisingą bylos nagrinėjimą ir veiksmingą teisinę gynybą (UNESCO, 2021, p. 22), tai siejama su atsakomybe bei atskaitomybe. Skaidrumo principu, literatūroje nurodoma, kad žmonės turėtų būti informuojami, kai yra priimamas sprendimas naudojantis DI paremtomis sistemomis (Ibarra, Douglas ir Tharmarajah, 2020, p. 9), o būtent DI subjektai yra įpareigoti užtikrinti, kad šie sistemų procesai būtų suprantami bei paaiškinami (UNESCO, 2021, p. 22). Paaiškinamumo principas bus išpildytas, kai netechniniais terminais bus paaiškinama, kaip algoritmai veikia, kokie duomenys yra naudojami ir kaip algoritmai numato teisingą prognozę (Egbert, 2019, p. 55).

Atsakomybė ir atskaitomybė turi remtis nacionaline bei tarptautine teise, o DI subjektai turėtų prisiimti atsakomybę, taip saugodami žmogaus teises bei laisves ir skatindami aplinkos bei ekosistemų apsaugą (UNESCO, 2021, p. 22). Nurodoma jog būtent atskaitomybė priklauso nuo to ar bus įgyvendinama sistemų stebėseną bei rizikų valdymas (Berryhill et. al., 2019, p. 109). Didelis dėmesys yra atkreipiamas ir atskaitomybės didinimui per auditų, partikrinimų bei priežiūros mechanizmus, o pačio audito atlikimo galimybė priskiriamos prie skaidrumo, teisingumo, lygybės bei jokios žalos principų (Jobin, Ienca ir Vayena, 2019, p. 7-10), todėl ši galimybė tampa ypač aktuali DI sistemų veikimo procese.

Sąmoningumo ir raštingumo principas skirtas, kad asmenys būtų apsaugoti nuo netinkamos informacijos, o supratimą apie DI technologijas ir duomenų reikšmę nurodoma skatinti per švietimą, t.y. per įvairius DI raštingumo mokymus, žiniasklaidą, valstybines institucijas, taip pat skatina įtraukti

lyderius iš privataus bei viešojo sektoriaus ir akademinės bendruomenės (UNESCO, 2021, p. 23). Manoma jog teisėjai bei teisės mokyklos turi didelį vaidmenį didinant DI specialistų informuotumą bei taip gerinant suvokimą apie esamus pokyčius bei galimybės praktiškai prisidėti (Europos veiksmingo teisingumo komisija, 2018, p. 9). Kompiuterinio raštingumo skatinimas taip pat kyla iš valstybės noro, jog visi asmenys turėtų lygias galimybes gauti technologijų naudą (Berryhill et. al., 2019, p. 20).

UNESCO, rekomendacijose išskyrė *Daugianario ir adaptyvaus valdymo bei bendradarbiavimo* principą, kuris nebuvo išskirtas nei mokslinėje literatūroje, nei kitų organizacijų rekomendacijose, kaip atskira sritis. Pagal šį principą valstybės remiantis tarptautine teise turėtų veiksmingai prižiūrėti bei reguliuoti duomenis, o sukurti ir priimti atviri DI standartai padėtų bendradarbiauti tarpusavyje (UNESCO, 2021, p. 23). Šiame principe atsiskleidžia idėja jog įvairūs suinteresuoti subjektai arba įvairios visuomenės grupės turėtų galimybę dalyvauti DI kūrimo ir diegimo procese per visą sistemos gyvavimo ciklą, tai leistų visiems dalytis nauda bei prisidėtų prie tvaraus vystymosi (UNESCO, 2021, p. 23), tam pritaria ir Europos veiksmingo teisingumo komisija (Europos veiksmingo teisingumo komisija, 2018, p. 9).

Apibendrinant galime įžvelgti jog tam tikri principai tampa kai kurių principų įgyvendinimo dalimi (pvz.: proporcingumo ir žalos vengimo principo įgyvendinimas yra saugumo ir apsaugos principo užtikrinimo dalis). Pastebėtina ir tai jog principuose atsikartoja vienokios ar kitokios naudos teikimas (pvz.: „užtikrinti technologijų naudos pasiekiamumą“, „sistemos turi teikti naudą žmonijai ir žemei...“, „visi asmenys turėtų lygias galimybes gauti technologijų naudą“). Galima pastebėti ir tai, jog tam tikri principai migruoja į kitus principus, pvz.: *žalos vengimo principas* pastebimas *saugumo ir apsaugos* dalyje „<...> vengti galimų pavojų <...>“. 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. Taip pat matoma jog tam tikri principai yra smarkiai susiję tarpusavyje, todėl įgyvendinant vieną privalu įgyvendinti ir kitą, tam kad principų sistema iš ties veiktų (pvz.: nediskriminavimo principą vargu ar įgyvendintume neužtikrinę duomenų apsaugos ar skaidrumo). Išplėtojant paskutiniąją mintį – nesant skaidrumo ir auditavimo galimybių šioje sferoje neužtikrinsime daugelio principų, t.y. jei duomenys nekokybiški, sistemos netvarios bei nesaugios jautriai informacijai saugoti, bus sunku nurodyti atsakomybę bei užtikrinti atskaitomybę. Šios sistemos gali teikti naudą tik tuo atveju jeigu bus laikomasi bendrų tarptautinių (mintyje turima DI kūrimo bei diegimo) standartų ir bus užtikrinta nuosekli sistemų priežiūra.

1.3. Galima dirbtinio intelekto žala teisėsaugos sistemoje

DI bruožų turinčios technologijos, turi tiek naudingų, tiek keliančių riziką aspektų. Atsižvelgiant į sistemų naudojimo sritį, t.y. teisėsaugos sistemą, svarbu išsiaiškinti, ką autoriai literatūroje įvardija, kaip galimą šių technologijų žalą, kurias sritis jos gali paveikti bei kokią įtaką gali padaryti teisėsaugos sektoriuje. Šioje dalyje pateikta informacija ne tik apie, tai kokios rizikos gali kilti pačios technologijos „viduje“, tačiau ir rizikos kurios atsiranda asmeniui naudojantis šiomis sistemomis.

Jungtinių tautų naujienlaiškyje, pristatant tarptautines DI etikos standartų rekomendacijas, panaudotas UNESCO pareiškimas, kad „Matome didėjantį lyčių ir etninį šališkumą, dideles grėsmes privatumui, orumui ir savarankiškumui, masinio sekimo pavojus, vis dažnesnį nepatikimų dirbtinio intelekto technologijų naudojimą teisėsaugos institucijose ir kt. <...>“ (United nations, 2021), todėl šiame bloke bus siekta detaliau panagrinėti galimas DI rizikas.

Duomenyse ar sistemų dizaine esantis šališkumas (Joh, 2018, p. 1142) paveiktų daug asmenų, kurie nėra nusikaltę arba yra iš marginalizuotų grupių (Moses ir Chan, 2018, p. 810; Joh, 2018, p. 1142), pvz.: JAV rizikos vertinimo įrankiais būdavo dažniau neteisingai apskaičiuota recidyvo rizika asmenims priskiriamiems mažumai negu daugumai (Sharma et. al., 2019, p. 8). Būdingas šališkumas gali sietis su skirtingais duomenų rinkimo metodais, policijos praktikom, lokacijos ir laiko aspektu, istoriniais įvykiais ar tam tikros grupės susidomėjimu (Ibarra, Douglas ir Tharmarajah, 2020, p. 11). Žinoma, nereikia atmesti galimybės jog asmenys programuodami algoritmus, ten gali perkelti savo šališkumus bei vertybes, taip sustiprinant stereotipus bei diskriminaciją (Wirtz, Weyerer ir Geyer, 2019, p. 605).

Kibernetinių atakų metu, užpuolikai gali įgauti prieigą ne tik prie žmogaus fizinės gyvenamosios vietos, tačiau kartu gali matyti ir visą nusikalstamumo istoriją (Wirtz, Weyerer ir Geyer, 2019, p. 603), vėliau galimai ja pasinaudoti, šantažuoti asmenis ir pan. Grėsmė asmens duomenų privatumui kyla ir tada, kuomet teisėsaugos institucijoms reikia papildomos informacijos apie asmenį, pvz.: renkant informaciją apie kaimynystę, stebint, apklausiant ar net įeinant į namų ar privačią virtualę erdvę (Degeling ir Berendt, 2018, p. 355).

Nurodoma, kad DI sistemos gali būti tiesiogiai nekontroliuojamos žmogaus, o tai lems atsakomybės atotrūkį – žmonės nebus atsakingi už šių sistemų elgesį, nes jų tiesiogiai nekontroliuoja ir nedaro joms įtakos (Wirtz, Weyerer ir Geyer, 2019, p. 603). Kartu šioje temoje išlieka žmogaus pakeitimo technologijomis grėsmė, todėl iškyla etinių problemų, susijusių su DI naudojimu (Vrontis et. al., 2022, p. 1245; Wirtz, Weyerer ir Geyer, 2019, p. 601).

Technologijų naudojimas gali sutrikdyti valdžią ir jos mechanizmus, kuriuos žmogaus teisių gynėjai ir pilietinės visuomenės organizacijos naudoja atskaitomybei skatinti (Land ir Aronson, 2020, p. 225). Naudojantis DI paremtomis priemonėmis iškyla klausimas, kas atsakingas už sistemos klaidas, ar asmuo, kuris priėmė sprendimą remiantis mašina, ar pati mašina, kuri sugeneravo tokį sprendimą? Kaip turėtų atrodyti procesas, paskutiniu atveju, kur asmuo sulaukia teisingumo ir žalos grąžinimo iš programos?

DI technologijos gali veikti taip, kaip žmogui sunku arba neįmanoma suprasti (Re ir Niederman, 2019, p. 262). Kai kurie autoriai nurodo jog savaime besimokančios DI programos gali tapti neprognozuojamos bei nebesivadovauti normatyviniu etiniu pagrindu (Wirtz, Weyerer ir Geyer, 2019, p. 604), tokiu atveju kiltu nenuspėjamas žalos kiekis. Pažymima, kad modelių išvestos prognozės turi būti vertinamos remiantis DI žiniomis bei praktine patirtimi, kitaip galima susidurti su iškreiptu tikrovės vaizdu (Meijer ir Wessels, 2019, p. 1036). Žinios reikalingos ir tam, jog sistemomis nebūtų pasitikima per daug, nes šios technologijos gali sukelti klaidingą saugumo jausmą (Završnik, 2021, p. 4).

Sistemos gali "per daug prisitaikyti" (ang. *Overfit*) prie turimų duomenų, o tai gali lemti neteisingus sprendimus, kai algoritmas bus taikomas kituose kontekstuose (Re ir Niederman, 2019, p. 270 – 271). Kadangi DI dažnai yra susijęs su prognozėmis, kai kurios iš jų neišvengiamai bus klaidingos (Joh, 2018, p. 1143; Re ir Niederman, 2019, p. 255), tokiu būdu perteklinį baudžiamąjį persekiojimą patirs nenusikaltę asmenys, o tuomet teisėsauga gali susidurti su visuomenės nepasitikėjimu.

Kompetencijų bei prieinamumo stoka nėra tiesioginė DI žala visuomenei, veikiau tai valstybės negebėjimo prisitaikyti prie tobulėjančių technologijų pasekmė, kuri gali pakenkti. Minima jog darbuotojai turės turėti reikiamų žinių ir įgūdžių, kad suprastų, kaip veikia DI sistema, tačiau autoriai nurodo jog institucijoms yra sudėtinga išlaikyti kompetencijas tolygiai su technologijų tobulėjimu (Berryhill et. al., 2019, p. 108). Asmenys neturintys tinkamų žinių, dirbdami, gali padaryti daug žalos negebėdami suprasti technologijų. Net jeigu DI taptų suvokiamas jis vis tiek išliktų potencialiai neprieinamas tiems, kurie neturi techninio išsilavinimo (Re ir Niederman, 2019, p. 264), kas sudarytų atskirtį visuomenėje.

Apibendrinant, dažniausiai minima žala yra galimas duomenų šališkumas bei duomenų apsaugos neužtikrinimas, per šiuos aspektus gali kilti diskriminaciją tam tikroms visuomenės grupėms arba asmenims ir taip pat rizika kiekvieno asmeninei informacijai. Svarbu pabrėžti jog žala gali atsirasti ne

tiesiogiai iš technologijų, o iš asmenų, kurie neturi pakankamai žinių, jog galėtų tinkamai su šiomis sistemomis dirbti. Žinoma, darbui reikalingas kompetencijų kėlimas, o jis nebūti visiems prieinamas, todėl kyla rizika visuomeninės atskirties padidėjimui. Šių sistemų klaidos gali būti itin skaudžios (pvz.: nuteistas nekaltas asmuo), tačiau tinkamai naudojamos jos gali atnešti didelę naudą visuomenei bei valstybei (pvz.: dėl DI paremto, puikiai veikiančio pinigų plovimo prevencijos mechanizmo į šalį yra pritraukiama daugiau investuotojų, taip keliant šalies ekonomiką). Pasikartojant – šių sistemų efektyvumas priklausys nuo to, kokie kokybiški duomenys bus joms pateikti (Karppi, 2018, p. 2).

1.4 Galima dirbtinio intelekto nauda teisėsaugos sistemoje

Nagrinėjant literatūroje nurodytas DI teisėsaugoje naudas tampa sudėtinga atskirti jas nuo tam tikrų technologijų, nes jų tikslas ir yra nauda. Nurodoma jog naudojami algoritmai bus tokie geri, kokia gera bus į juos patenkanti informacija (Karppi, 2018, p. 2), todėl svarbu atkreipti dėmesį, kad tinkamai įdiegtos DI programos daugelio aukščiau išvardytų grėsmių gali neturėti (pvz.: diskriminacijos galimybė, duomenų nesaugumas ir pan.). Šios programos galėtų užtikrintų saugumą ir lygybę teisėsaugos procesuose procesuose, pvz.: naudojant identišką algoritmą nagrinėjant teisminius ginčus, DI gali sušvelninti ar net panaikinti galimą žmogiškąjį šališkumą, užkertant kelią pasirinkto „gero“ teisėjo savivalei (Re ir Niederman, 2019, p. 256). Šioje dalyje tampa aktualu toliau panagrinėti DI naudą.

Teisėsaugos gaunamų ir analizuojamų duomenų kiekis dar niekada nebuvo toks didelis, pvz.: JK nutrauktos iššaginimo bylos, dėl policijos nesugebėjimo rasti svarbių įrodymų, tarp didelio kiekio "Facebook" ir kitų socialinėse medijose esančių pranešimų (Casey, Burrell ir Sumner, 2019, p. 104), todėl čia svarbų vaidmenį atliktų pagalbinė įranga. 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 policijos pajėgoms užtruktų daug ilgiau ir tikėtina atneštų mažiau naudos. Taip pat programos suteikia galimybė atlikti auditą, nuoseklumo ir kontrolės bei veiklos stebėseną (Ibarra, Douglas ir Tharmarajah, 2020, p. 23), kas skatina sistemų tobulinimą bei visuomenės pasitikėjimą jomis.

DI paremtų priemonių naudojimas gali būti naudingas norint mažinti nusikaltimų skaičių ir užtikrinant saugumą miestuose, kai kurie atvejai JAV rodo, kad naudojant prognozuojamąją policijos veiklos programinę įrangą, nusikalstamumas sumažėja (Meijer ir Wessels, 2019, p. 1031; Joh, 2018, p. 1139). Teisėsaugoje naudojami prognozavimo metodai padeda nustatyti asmenis, kurie potencialiai gali būti įtraukti į nusikalstamą veiką – kaip aukos, arba kaip nusikaltėliai (Meijer ir Wessels, 2019, p. 1034).

DI priemonės gali prisidėti prie mediacijos teisminiame procese įgyvendinimo, su teisėjo galimybe naudoti programą ne visam procesui atlikti, o dėl tam tikrų tikslių bylos detalių nustatymo, pvz.: pakartotinio nusikalstamumo rizikos (Europos veiksmingo teisingumo komisija, 2018, p. 54), ši galimybė suteiktų reikiamą autonomijos jausmą (teisėjui ir proceso dalyviams). Tam tikros DI programos gali pagerinti pareigūnų darbo efektyvumą vietoje ir laike, nes jie gali geriau reaguoti į nusikalstamą veiklą ir lengviau surasti įtariamuosius pvz.: programinės įrangos pagalba atpažįstant valstybinius numerius; turint sudarytą efektyviausią patruliavimo maršrutą mieste (Meijer ir Wessels, 2019, p. 1034) ir pan. Šios priemonės gali optimizuoti darbuotojų darbą perkeldamos jų pastangas nuo kasdienių biurokratinių užduočių prie didesnės vertės veiklos, pvz.: gali padėti tyrėjams efektyviau atsakyti į asmenų užklausas dideliuose duomenų rinkiniuose rasdamas medžiagą tenkinančią pačią užklausą (Casey, Burrell ir Sumner, 2019, p. 104). Taip pat nurodoma, kad DI „gali atlaisvinti beveik trečdalį valstybės tarnautojų laiko vos per kelerius ateinančius metus“ (Berryhill et. al., 2019, p. 123) leidžiant sutaupyti laiko ir sumažinti darbuotojams naštą (Aoki, 2021, p. 3).

Apibendrinant, beveik vienareikšmė didžiausia DI nauda yra galimybė pagreitinti procesus bei veiksmingiau išnaudoti turimus teisėsaugos resursus finansine, laiko, bei darbuotojų prasme. Svarbu susieti su pirmojoje šio darbo dalyje išsakyta mintimi jog DI gali kai kuriais atvejais pralygti žmogaus sugebėjimus, todėl duomenų analizei šie įrankiai tampa ne tik naudingi laiko bet ir kokybės atžvilgiu. Aktualu pabrėžti jog sudarius rizikos valdymo priemones, teisingai kuriant bei diegiant DI galimos rizikos ir žala sumažėja ir tuomet galime naudotis plataus pobūdžio technologijų teikiama nauda. Auditavimas, tobulinimas ir šių sistemų priežiūra gali panaikinti ne tik šališkumą teisėsaugos veikloje tačiau ir geriau apsaugoti mūsų duomenis bei pagreitinti policijos veiklą.

2. Dirbtinio intelekto naudojimas teisėsaugoje – atvejų analizė

2.1. Tyrimo metodika

Tyrimo problemos: Analizuojant mokslinės literatūros plačiai aprašytus DI etikos principus, kyla tiesioginis klausimas, kaip šie principai skiriasi tarpusavyje tiriamose šalyse bei kokie yra matomi esminiai dėsningumai. Šį klausimą spręsti padės įsigilinimas į TPŠ DI strategijas, veiklos planus bei ataskaitas.

Teorinėje dalyje pateikiamos šių programų naudos bei grėsmės suteikė platų žinių lauką, tačiau nesudarė jokio vaizdo, kaip šalys išskiria žalos bei naudos galimybes naudojant DI technologijas. Tai atsiskleis analizuojant TPŠ DI strategijas, veiklos planus bei ataskaitas.

Literatūroje aprašančioje DI etikos principus vienas iš išryškintų faktorių buvo asmens vaidmuo visame sistemų gyvavimo cikle, kas iš esmės nurodo žmogaus svarba ne tik kuriant, bet ir diegiant bei prižiūrint programas. Šio tyrimo kontekste svarbu, kiek įmanoma, labiau išsiaiškinti ar šalys akcentuoja į žmogų orientuoto DI taikymą ir jei taip, kaip tai pabrėžia bei išsireiškia tiek savo šalies DI strategijoje, tiek šaltiniuose aprašančiuose naudojamas DI sistemas.

Kadangi viena iš labiausiai žinomų šių technologijų grėsmių yra duomenų apsaugos pažeidimai, o teorinėje prieigoje apie teisinę šios srities padėtį nebuvo išsiplėsta, tampa aktualu aptarti bei palyginti tarpusavyje, kaip šalys užtikrina duomenų apsaugą bei kokie įstatymai daugiausiai figūruoja analizuojamoje literatūroje.

Teorinė darbo dalis suteikė abstrakčius DI technologijų naudojimo teisėsaugoje būdus, todėl tyrime svarbu aptarti, kokios technologijos yra randamos viešai prieinamoje informacijoje, tiriamų valstybių rėmuose, kaip šios sistemos skiriasi (ar skiriasi?), bei į kokios krypties sistemas šalys daugiausia orientuojasi.

Tyrimo tikslas – palyginti technologiškai pažangių šalių viešai prieinamą informaciją apie DI taikymą bei naudojimą teisėsaugoje.

Tyrimo klausimai:

1. Kaip skiriasi arba sutampa DI etikos principai, galimos naudos bei žalos lyginant TPŠ DI strategijas – veiklos ataskaitas – planus?
2. Kaip yra atskleidžiamas ir/ ar pabrėžiamas į žmogų orientuoto DI naudojimas?
3. Kaip yra užtikrinamas šių sistemų saugumas šalyse bei į kokius duomenų apsaugos įstatymus referuojama dažniausiai kai kalbama apie DI?

4. Palyginti kaip TPŠ skirtingai arba dėsningai naudoja DI teisėsaugos sistemoje?

Tyrimo metodas. Siekiant susidaryti detalų temos vaizdinį pasitelkiamas keletos atvejų analizės metodas (ang. *Multiple case study*) (Johansson, 2007; Rashid et. al., 2019; Tellis, 1997), kuris leis iš didelio medžiagos kiekio išanalizuoti ir tarpusavyje palyginti temai aktualius, aspektus. Keletos atvejų analizės metodo stiprioji pusė yra galimybė analizuoti įvairaus tipo informaciją siekiant atrasti bendrus dalyko principus. Siekiant užtikrinti duomenų patikimumą pasitelkiama įvairaus tipo medžiaga: tarptautinių organizacijų dokumentai, mokslinė literatūra, nacionaliniai šalių dokumentai, teisės aktai bei DI organizacijų publikacijos, kurias vėliau pagal konkretų tikslą bus sugretinamos, palyginamos ir apibendrinamos. Taipogi, šiame tyrime pasirinktų šalių kiekis bei geografinė padėtis, suteiks didelės vertės, nes leis daryti apibendrinančias išvadas apie TPŠ patirtį taikant tokio tipo technologijas teisėsaugoje. Svarbu ir tai jog tarp šalių atliekama lyginamoji analizė suteiks galimybę atrasti dėsningumus ir skirtumus šioje srityje, kurie gali pasitarnauti norint teikti rekomendacijas šalims, kurios siekia modernizuoti teisėsaugos procesus. Taip pat tyrimas suteiks žinių pagrindą apie esama DI teisėsaugoje situaciją tiriamose šalyse.

Šalių atranka. Šiame tyrime buvo taikoma tikslinė atranka. Kaip TPŠ, buvo pasirinktos: Jungtinės karalystės (JK), Belgija, Vokietija, Prancūzija bei Estija. Šalių pasirinkimą lėmė dažnas pasikartojimas analizuojamoje literatūroje. Šios valstybės nurodomos, kaip inovatyvios bei didelį dėmesį skiriančios technologiniui valstybės vystymuisi (*žiūrėti 1 priedą dėl detalesnio šaltinių sąrašo, kuriuose akcentuojamas šalių pažangumas DI naudojimo srityje*).

- **Estija** (Boahemaa, 2019; Berryhill et. al., 2019; Campbell, 2020; Europos taryba, 2018; Europos taryba, 2021);
- **UK** (Oswald et. al., 2018; Leslie, 2019; Oswald et. al., 2018; UNICRI ir INTERPOL, 2020);
- **Belgija** (Lyuben et. al., 2021; Walker-Osborn ir Chan, 2017; Europos parlamentas, 2020; Deloitte, 2020; Europos taryba, 2021);
- **Prancūzija** (Christakis ir Trotry, 2020; European digital rights, 2020; Jobin, Ienca ir Vayena, 2019; Europos parlamentas, 2020; CNIL, 2019; CEPEJ, 2018);
- **Vokietija** (Gerstner, 2018; Egbert, 2018; Egbert ir Krasmann, 2020; Europos taryba, 2018; European digital rights, 2020).

Šalys pasirinktos ir dėl savo geografinės padėties, kuri leis susidaryti bendresnį Europos geografinėje zonoje esančia padėtį DI taikymo teisėsaugoje kontekste bei suteiks galimybę daryti

apibendrinančias išvadas. Tai tampa ypač svarbia detale tyrimo kontekste, kadangi ši informacija gali būti naudinga kitoms valstybėms siekiančioms tobulinti DI taikymo bei naudojimo ypatumus teisėsaugos sistemoje.

1, 2, ir 3 klausimo išpildymo strategija. Siekiant atsakyti į šiuos klausimus bus analizuojamos naujausiai išleistos nacionalinės TPŠ DI strategijos, ataskaitos bei planai. Šių trijų dokumentų pasirinkimas yra būtinas, nes ne visos tyrime pasirinktos šalys išleidžia strategijas. Ataskaitos ir planai yra tiesiogiai su DI taikymu bei diegimu susiję nacionaliniai dokumentai, todėl jų analizė tarpusavyje neturėtų sutrukdyti atliekamam tyrimui. Taip pat iš šių dokumentų svarbu atsakyti ir į 2-ajį bei 3-iajį klausimus, kadangi svarbu nurodyti kiek ir kaip yra aprašoma duomenų apsauga bei į žmogų orientuoto DI naudojimas nacionaliniuose šalių dokumentuose. Ši informacija parodys tam tikrą šalies požiūrį į komunikaciją bei norimą DI kryptį.

3, 4 klausimo išpildymo strategija. Atsakant į 3-ajį klausimą, naudojama literatūra persidengia su 4-uoju kadangi aprašant naudojamas technologijas gali būti užsiminta arba referuojama į tam tikrus teisės aktus užtikrinančius duomenų apsaugą. Siekiant atsakyti į 4-ąjį klausimą bus naudojama įvairaus tipo, viešai prieinama informacija apie šalių naudojamas DI technologijas teisėsaugos sistemoje. Būtent dėl tyrimo apribojimų bus siekiama išanalizuoti kuo įvairesnio tipo informacijos šaltinius, tokiu būdu tiriant optimaliai didelį informacijos kiekį.

Informacija iš nagrinėjamų šaltinių buvo renkama atitinkamai pagal uždavinio tikslą bei grupuojama microsoft excel programoje. 1, 2, ir 3 klausimams atsakyti buvo pasirinktos naujausiai išleistos šalių DI strategijos, planai arba ataskaitos. Dėl 1-ojo ir 2-ojo klausimo buvo sukurti kodai, kurie padėjo geriau suskirstyti dokumentuose esančią informaciją (*žiūrėti 2 priedą*), nors ne visi kodai tiesiogiai susiję su klausimų tikslu, jie pasirinkti dėl platesnio vaizdo susidarymo. 4-ojo klausimo atsakymui visus analizuotus šaltinius galima pamatyti 3 priede – kiek ir iš kokių šaltinių buvo surastos naudojamos DI priemonės teisėsaugos sistemoje (šioje dalyje buvo nagrinėti 44 šaltiniai), taip pat juose buvo siekiama atrasti informacijos susijusios ir su 3-iuoju klausimu apie į žmogų orientuoto DI svarbą.

Tyrimo apribojimai. Svarbu pabrėžti, jog lyginant tam tikrą atvejį skirtingose šalyse, gali kilti rizika informacijos lyginimo procese. Tam tikri dokumentai leidžiami nacionaliniu lygmeniu gali skirtis savo struktūra bei apimtimi nuo kitos šalies leidinių, taip pat vienos šalys gali turėti aktyvesnę komunikaciją už kitas, o tai lems duomenų persvara tarp šalių. Tačiau šio tyrimo metodo pagalba, šias galimas rizikas siekiama suvaldyti pasitelkiant pagalbinius mokslinius bei su DI susijusių organizacijų publikuojamus leidinius. Taip pat šio tyrimo tema sudaro sunkumų rasti viešai prieinamos informacijos

apie visas teisėsaugoje taikomas DI technologijas, nes tokios informacijos viešinimas gali kelti pavojų šalies saugumui.

2.2. Dirbtinio intelekto etikos principai, nurodoma žala bei nauda lyginant tiriamų šalių DI strategijas

Šioje darbo dalyje analizuojamos TPŠ DI strategijos bei joms prilyginami dokumentai įtvirtinantys šalyje taikomo DI principus. Taip pat iš dokumentuose esančios informacijos išskirtos šalių nurodomos šių technologijų naudos bei galimos žalos. Šių dokumentų analizė leido įsižiūrėti į valstybių požiūrį bei tam tikra prasme taktiką DI taikymo rėmuose. Šiame skyriuje galime pamatyti, kokią informaciją nagrinėjamos šalys pateikia visuomenei.

Principai. Visos šalys įvardydamos DI principus paminėjo saugumo, patikimumo, skaidrumo, duomenų apsaugos, nediskriminavimo aspektus (Vokietijos federalinė vyriausybė, 2020, p. 5, 21; AI-4Belgium, 2021, p. 8, 14, 15; Estijos respublikos vyriausybė, 2019, p. 41, 42; Prancūzijos vyriausybė, 2021b, p. 3,4; Jungtinės karalystės vyriausybė, 2021, p. 46, 56, 59). Bendradarbiavimo principą išskyrė Vokietija bei Belgija (Vokietijos federalinė vyriausybė, 2020, p. 9; AI-4Belgium, 2021, p. 8) (*žr. 1 lentelę*). Vokietija bei JK vienintelės savo strategijose akcentavo poreikį įtraukti į sistemų kūrimo ir diegimo procesą, kuo įvairesnių grupių asmenis, taip praplečiant reikalingas žinias, poreikius bei patirtis (Vokietijos federalinė vyriausybė, 2020, p. 25; Jungtinės karalystės vyriausybė, 2021, p. 17) šis požiūris mokslinėje literatūroje labai girtinas bei skatinamas, siekiant pašalinti šališkumą rasės, lyties ar kitų jautrių grupių pagrindu.

Principai	JK	Belgija	Prancūzija	Estija	Vokietija
Saugumas	+	+	+	+	+
Patikimumas	+	+	+	+	+
Skaidrumas	+	+	+	+	+
Duomenų apsauga	+	+	+	+	+
Nediskriminavimas	+	+	+	+	+
Autonomija			+	+	
Duomenų tvarkymo minimumas			+	+	
Bendradarbiavimas		+			+
Komandų įvairovė sistemų kūrimo procese	+				+
Atsekamumas		+			+

Randamumas		+			+
Duomenų prieinamumas		+			+

1 Lentelė ***„Šalių išskiriamų principų bendrumas bei išskirtinumas“.***

Estija bei Prancūzija išsiskyrė paminėdamos duomenų tvarkymo minimumo principą (Estijos respublikos vyriausybė, 2019, p. 41), bei autonomijos reikalingumą (Estijos respublikos vyriausybė, 2019, p. 42, Prancūzijos vyriausybė, 2021c, p. 2).

Vokietijos DI strategijoje, kaip vienas iš principų buvo nurodomas sprendimų patikimumas bei jų atsekamumas ir prieinamumas per visą jų gyvavimo ciklą (Vokietijos federalinė vyriausybė, 2020, p. 24), tai išsiskyrė iš nagrinėjamų šalių, kadangi toks požiūris paliečia daugelį DI principų bei užtikrina auditavimo bei nuolatinio patikrinimo galimybes.

Belgija akcentavo duomenų randamumo, prieinamumo, jų pakartotinio naudojimo svarbą (AI-4Belgium, 2021, p. 16), o tai netiesiogiai akcentuoja skaidrumo, aiškumo bei tvarumo principus atskleistus teorinėje dalyje.

Šie duomenys atskleidžia jog visos šalys mini pagrindinius principus, kurie saugo jautriausias sritis (pvz.: skaidrumas, duomenų apsauga, nediskriminavimas), kurios visuomenėje susilaukia daug dėmesio, o šių principų nesilaikymas tiesiogiai gali sukelti daug žalos. Šalys išsiskiria pavieniais principais, tokiais kaip bendradarbiavimas, komandų įvairovė sistemų kūrimo procese, duomenų prieinamumas, kurie iš esmės nesusilaukia didelio dėmesio visuomenėje, tačiau mokslinėje literatūroje šie principai yra itin svarbūs visame technologijų gyvavimo cikle.

Nauda. Bendra visų šalių išskirta nauda buvo viešųjų paslaugų patobulinimas (žr. *2 Lentelę*). Prancūzijos, Estijos bei Belgijos DI strategijose jis buvo daugiausiai išplėstas bei išsamiau papildytas. Prancūzai nurodė jog „<...>naudojant DI atsilaisvina darbuotojų laikas didesnės pridėtinės vertės užduotims ir geresnei pagalbai naudotojams.“ (Prancūzijos vyriausybė, 2021a, p. 2), Estai su tuo pačiu požiūriu pridūrė, kad rutininės ir automatizuojamas užduotis reiktų palikti įrangai (Estijos respublikos vyriausybė, 2019, p. 17), o siejant tai su teorine medžiaga daroma prielaida jog toks požiūris atspindi norą panaudoti šio tipo technologijas srityse, kur jų našumas bus efektyviausias. Tuo tarpu belgai nurodė, kad šios technologijos gali išlaisvinti bei suteikti laiko žmogiškiems dalykams – šeimai, kūrybai bei laimės siekimui (AI-4Belgium, 2021, p. 2), kas kelia klausimą ar tai siekis įsiteigti visuomenei, ar kryptingas judėjimas į žmogų orientuoto DI diegimą?(strategijoje ši kryptis nėra nurodoma)

Naudos	JK	Belgija	Prancūzija	Estija	Vokietija
Viešųjų ryšių tobulinimas	+	+	+	+	+
Gynybos sektorius	+				+
Policijos veikla ir saugumas					+
DI naudos įvairovė		+			
Žmogaus teisių sauga			+		

*2 Lentelė **„Šalių išskiriamų naudų bendrumas bei išskirtinumas“.** Geltonai pažymėti langeliai nurodo valstybes, kurios išsiskyrė informacijos gausa aprašydamos atitinkamą DI naudą.*

JK bei Vokietija vienintelės iš nagrinėjamų šalių rašydamos apie DI sistemų teikiamą naudą paminėjo jų panaudojimą gynybos srityje (Jungtinės karalystės vyriausybė, 2021, p. 47; Vokietijos federalinė vyriausybė, 2020, p. 18, 22). Tai nurodo JK ir Vokietijos tam tikrą prioritetą šalies gynybai bei orientaciją į šalies saugumą. Galime daryti prielaidą jog šios šalys mato potencialią naudą taikyti DI technologijas šioje srityje bei skiria tam daug finansinių resursų.

Vokietija daugiausiai iš visų nagrinėjamų TPŠ prasiplečia apie DI naudą saugumo bei policijos veiklos kontekste. Nurodo jog šios sistemos gali padėti sustiprinti esamus pajėgumus ir padaryti policijos darbą tikslingesnį ir veiksmingesnį bei sumažinti pareigūnams tenkančią psichologinę įtampą (Vokietijos federalinė vyriausybė, 2020, p. 22). Taip pat Vokietija pažymi, kad kiekvienu konkrečiu atveju reikia numatyti, kaip DI panaudojimas policijoje gali pažeisti žmonių teises (Vokietijos federalinė vyriausybė, 2020, p. 22).

Belgų DI strategija išskirtinė tuo, jog joje nurodoma daug konkrečių sričių, kur šio tipo technologijos gali teikti naudą, pvz.: „Kurtieji vaikai gali sekti pamokas kartu su bendraamžiais konvertuodami kalbą į tekstą“ (AI-4Belgium, 2021, p. 4), „Teisininkai naudosis DI, kad rastų atitinkamus teisės aktus; gydytojai – kad padėtų diagnozuoti ligas...“(AI-4Belgium, 2021, p. 12), tačiau nenurodo ar šios paslaugos yra teikiamos Belgijoje, ar tai tėra hipotetinė minimų technologijų nauda.

Iš 2 lentelėje pateiktų duomenų Estija išlieka vienintelė valstybė, kurios DI strategijoje nurodyta viena šių technologijų nauda. Vokietija tuo tarpu pirmauja įvardydama tris sritis kuriose DI gali pasitarnauti. Lyginant šiuos duomenis su teorinėje dalyje aptariamomis DI naudomis, matomas ryškus skirtumas – nagrinėjamos šalys išskiria mažą kiekį DI naudų, dėl šio aspekto visuomenė gali susidaryti iškreiptą DI potencialą. Galima kelti prielaidą jog šalys nurodo tik tuos aspektus, kuriais tvirtai tiki ir kuriuose siekia diegti šias sistemas, tačiau tokiu atveju, tai yra labai siauros DI panaudojimo ribos.

Galimos grėsmės bei žalos. Kitaip nei kitose dalyse, šioje – nebuvo galima išskirti bendros šalių nurodomos DI technologijų rizikos. Išskyrus JK, tyrime nagrinėjamos šalys DI strategijose nesuteikė daug dėmesio galimų grėsmių aprašymui.

JK ir Vokietija pažymėjo svarbą nustatyti, kuriose srityse, kokios grėsmės gali kilti (žr. 3 lentelę). Rizikų gali ir nebūti jeigu pramoninis DI nenaudoja asmens duomenų (Vokietijos federalinė vyriausybė, 2020, p. 25), tai nurodo įdomų Vokietijos požiūri, kadangi iš teorinės darbo dalies žinome jog šios technologijos gali sukelti grėsmę ne tik asmens duomenims, tačiau ir įmonės ar organizacijos resursams (dėl technologinių spragų atsirandanti našumo stoka, piniginis nuostolis, vėluojančios prekės).

JK vienintelė iš nagrinėjamų šalių ryškiai akcentavo skaidrumo, duomenų reprezentatyvumo bei šališkumo aspektus (Jungtinės karalystės vyriausybė, 2021, p. 31, 51), o tai iš esmės mokslinėje literatūroje plačiausiai aprašomi, kaip nerimą keliantys, veiksniai. JK taip pat mini ir atskaitomybės keblumus tačiau Estija šiuo klausimų išsiplečia ir nuodugniai aprašo kylančius sunkumus, kas iš esmės nurodo šalies norą sukurti kokybišką sistemų stebėseną bei rizikų valdymą (Berryhill et. al., 2019, p. 109). Estija nurodo jog „Gamintojas atsako už žalą, padarytą dėl jo gaminio trūkumų, t.y. jam taikomos griežtesnės atsakomybės taisyklės“(Estijos respublikos vyriausybė, 2019, p. 40).

Prancūzija išskirtinai pabrėžia jog DI grįstos programos padės apsaugoti bei stiprinti pagrindines teises prie kurių prisirišusi jų valstybė (Prancūzijos vyriausybė, 2021b, p. 2), tačiau šių teisių tiksliai neįvardina. Prancūzija nenurodė nei vieno aspekto apie galimas DI technologijų grėsmes, kas sukuria iškreiptą vaizdą ir atskleidžia tam tikras komunikacijos spragas.

Grėsmės	JK	Belgija	Prancūzija	Estija	Vokietija
Grėsmių nustatymas atsižvelgiant į skirtingas naudojimo sritis	+				+
Atskaitomybė *(kyla neaiškumų kas atsakingas už DI žalą)*	+			+	
Skaidrumas	+				
Nepasitikėjimas teisėsaugos sistema		+			
Duomenų reprezentatyvumas	+				
Šališkumas	+				
Nenurodo grėsmių			+		

3 Lentelė „***Šalių išskiriamų grėsmių bendrumas bei išskirtinumas“***

Belgija pažymi jog DI gali kelti pasitikėjimo ir etinių klausimų, strategijoje taip pat nurodo jog nuo duomenų gali priklausyti tinkamas arba kenksmingas nusikalstamumo nustatymas ir policijos veikla (AI-4Belgium, 2021, p. 14), o tai gali padaryti daugiausiai žalos ne tik konkretaus asmens gyvenimui (pvz. nepelnytas bausmės paskyrimas), tačiau ir visuomenės pasitikėjimui teisėsaugos sistema.

Vokietija strategijoje nurodė jog grėsmių galima išvengti nustatant konkrečias DI sistemų kūrimo ir naudojimo taisykles bei parengus patikimus DI principus, suderintus visoje ES (Vokietijos federalinė vyriausybė, 2020, p. 23), tai atskleidžia tam tikrą leidėjų požiūrį, kuris siekia daugiau nuraminti visuomenę nurodydamas sprendimo būdus, o ne įvardydamas kylančias grėsmes.

Iš 3 lentelės duomenų matomas aiškus JK pranašumas nurodant DI galimas grėsmes, tuo tarpu kitos šalys nurodo tik po vieną galimą riziką, o Prancūzijos atveju jos iš vis nėra nurodomos. Galima kelti prielaidą jog daugumą šalių baiminasi išskirti galimas DI technologijų rizikas dėl galimai visuomenėje kilsiančios panikos. Dėl šios priežasties, kai kurios šalys, tokios kaip JK ir Vokietija, minėdamos galimas rizikas stengiasi kartu nurodyti jų valdymo būdus.

Apibendrinant visą skyrių, nagrinėjamos TPŠ DI strategijos, atskleidė jog visos šalys daugiau ar mažiau yra linkusios tiksliai išskirti galimą naudą ir blankiai aprašyti galimas grėsmes. Matoma didesnė koncentracija į rizikų prevencija negu į jų įvardinimą, o tai gali būti susiję su nenoru baiminti visuomenės. Taip pat išsiskiria JK bei Vokietijos tendencija – įvardinti principus per vertybių, siekių, taisyklų prizmes. Strategijose minimi principai daugiausia išlieka vienodi. Kartojasi tie principai, kurie liečia jautriausias temas visuomenėje (šališkumas, diskriminacija, skaidrumas), šalys išsiskiria pavienių principų nurodymų, kurie liečia mokslinėje literatūroje nurodytas svarbias sritis tačiau visuomenėje jos susilaukia mažo dėmesio.

2.3. Į žmogų orientuoto dirbtinio intelekto svarba tiriamose valstybėse

Nei vienoje iš nagrinėjamų strategijų, ataskaitų ar veiklos planų nebuvo apibrėžiamas ir nagrinėjamas į žmogų orientuoto DI naudojimas. Skirtingai, nei rekomenduojama literatūroje, tik trys šalys paminėjo jog reiktų „užtikrinti, kad DI būtų orientuotas į žmogų“ (Estijos respublikos vyriausybė, 2019, p. 42), bei skatinti į žmogų orientuoto DI kūrimą ir diegimą (AI-4Belgium, 2021, p. 7; Vokietijos federalinė vyriausybė, 2020, p. 24-25). Vienintelė Vokietija išsiskyrė paminėjusi planą įkurti DI

observatoriją, kuri stebės tendencijas ir rengs galimus sprendimus bei rekomendacijas dėl į žmogų orientuoto DI dizaino (Vokietijos federalinė vyriausybė, 2020, p. 20), kas iš esmės nurodo suinteresuotumą šioje srityje.

Skaitant apie DI priemones arba joms taikomus teisės aktus, ar kitas rizikos valdymo priemones, nebuvo aptikta jokios tiesioginės nuorodos į žmogų orientuoto DI taikymą. Tik Vokietijos atveju, nagrinėjant DI taikomas apsaugos priemones, buvo galima įžvelgti netiesioginę nuorodą į šią kryptį (*ši mintis akcentuota 3.4 skyriuje*), tačiau tai nesuteikia jokių tvirtų indikacijų apie šalies polinkį vadovautis šiuo požiūriu.

Tokie atradimai suponuoja dvi prielaidas, pirmoji – šalys nemato poreikio teikti daugiau dėmesio skelbiant apie šia galimą DI taikymo kryptį, antroji – nagrinėjamos šalys nėra pakankamai susipažinusios su į žmogų orientuoto DI kryptimi bei nemato joje potencialo.

2.4. Dirbtiniam intelektui taikomi teisės aktai bei kiti apsaugos būdai tiriamose šalyse

Daugelyje šaltinių vienas iš pirmųjų įstatymų, kurie yra minimi kalbant DI tematika – BDAR (Bendrasis duomenų apsaugos reglamentas), tai europinio lygmens įstatymas, kuriuo yra nustatomos taisyklės susijusios su fizinių asmenų apsauga tvarkant jų duomenis bei laisvu asmens duomenų judėjimu (BDAR, 1str.). Šis įstatymas galioja ne tik visoms Europos sąjungos narėms tačiau ir Europos ekonominei sąjungai.

Belgijos atveju aiškiai nurodoma, kad policijos vykdomai prognozuojamajai veiklai BDAR įstatymas nėra taikomas (Lyuben et al., 2021, p. 47). Belgijoje „Svarbiausias automatizuotą sprendimų priėmimą reglamentuojantis teisės aktas yra Duomenų apsaugos reglamentas“ (Automating society 2019 - Belgium). Taip pat nurodo jog būtent policijoje renkamų duomenų atvejui yra taikomi: Policijos tarnybos įstatymas, Integruotas policijos įstatymas, BPK, EP reglamentas (2016/679) dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir 2018 m. liepos 30 d. įstatymas dėl fizinių asmenų duomenų apsaugos (Lyuben *et al.*, 2021, p. 50) (*žr. 4 lentelę*), tačiau niekur nėra grindžiama, kaip tiksliai šie įstatymai užtikrina asmenų teises ir saugumą naudojantis DI paremtomis technologijomis.

Šalis	**Įstatymai bei reglamentai susiję su DI veikla**
Belgija	Duomenų apsaugos reglamentas
	BDAR
	Policijos tarnybos įstatymas

	Integruotas policijos įstatymas
	Baudžiamojo proceso kodeksas
	Europos parlamento reglamentas (2016/679) dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo
	2018 m. liepos 30 d. įstatymas dėl fizinių asmenų duomenų apsaugos

4 lentelė ***„Belgijos įstatymai bei reglamentai susiję su DI veikla“***

Yra papildoma jog policijos veiklą, kuri liečia asmenų duomenis, prižiūri duomenų apsaugos pareigūnai, federalinės ir vietos policijos generalinė inspekcija ir taip pat nepriklausomos įstaigos, tačiau nėra papildoma, kaip tai tiesiogiai arba netiesiogiai apsaugo galimą DI sistemų žalą.

Tarptautinė advokatų asociacija 2020 m. leidinyje nurodo jog šiuo metu **Prancūzijoje** nėra sukurtų konkrečių taisyklių skirtų tik DI, jam taikomi kitų esančių reglamentų segmentai, o 2022 m. leidinyje tikina jog atsiranda reglamentų, kurie apima bendrą DI arba MM sistemų naudojimą, bet tokį reguliavimą diegia ES, o ne Prancūzija. Abiejuose minėtuose leidiniuose pirmieji įstatymai nurodomi BDAR bei Prancūzijos 1978 m. sausio 6 d. įstatymas Nr. 78-17 dėl informacinių technologijų, duomenų rinkmenų ir pilietinių laisvių (International Bar Association, 2020, p. 63; International Bar Association, 2022, p. 66) (*žr. 5 lentelę*). „Prancūzijos duomenų apsaugos įstatymas oficialiai kontroliuoja algoritminius sprendimus <...> (International Bar Association, 2022, p. 66) bei nurodo, kad joks teisines pasekmes sukeliantis sprendimas negali būti priimtas remiantis automatizuotu asmens duomenų tvarkymu.

Šalis	**Įstatymai bei reglamentai susiję su DI veikla**
Prancūzija	BDAR
	1978 m. sausio 6 d. įstatymas Nr. 78-17 dėl informacinių technologijų, duomenų rinkmenų ir pilietinių laisvių (Duomenų apsaugos aktas)

5 lentelė ***„Prancūzijos įstatymai bei reglamentai susiję su DI veikla“***

Nors Prancūzijos duomenų apsaugos įstatymas kartu su BDAR draudžia priimti automatizuotus individualius sprendimus šalyje yra keletas išimčių. Skaitmeninės respublikos įstatymu leidžiama priimti sprendimus naudojant algoritmus jeigu yra pateikta suinteresuotos šalies informacija – šioje vietoje nėra prasiplečiama, kokios būtent informacijos reikalaujama, bei kiek plačiai šį įstatymą galima pritaikyti ir vartoti. Kita išimtis yra žvalgybos agentūrų srityje, jos naudodamos ryšio duomenis siekia aptikti terorizmo rizikas. Skaitant apie naudojamas DI sistemas Prancūzijoje, galima atrasti ir kylančių

etinių/ moralinių klausimų, ar duomenys tinkami/ proporcingi ir ar jų saugumas pakankamas? Tai reiškia, kad gali būti teisėtų ir pagrįstų atvejų, kai reikia naudoti veido atpažinimą, tačiau ne visais atvejais jis turėtų būti laikomas pageidaujamu ar įmanomu (CNIL, 2019, p. 5). Šis požiūris nurodo tam tikrą šalies poziciją dėl DI naudojimo – siekiama apriboti jo naudojimo galimybes, taip išvengiant galimų rizikų ar privatumo pažeidimų.

JK kaip ir kitos šalys pirmiausia mini BDAR (*žr. 6 lentelę*), tačiau po „Brexit“, šio įstatymo, bei duomenų apsaugos įstatymo, galią norima mažinti, taip silpninant visą duomenų apsaugos rėžimą (Roberts, Babuta, Morley, et. al., 2022, p. 5-6). Tokiais veiksmais norima suteikti daugiau laisvės inovacijoms bei duomenų sklaidai, tačiau tai kelia didelę riziką ir parodo šalies nesuinteresuotumą etikos bei žmonių teisių aspektais, atsižvelgiant ir į tai jog projekte dalyvavę konsultantai dauguma prieštaravo tokiems pakeitimams. Šie procesai iškelia klausimą ir autoriams, ar pakeitimai atitiks ES standartus ir ar duomenys tarp ES ir JK galės judėti laisvai?

Šalis	Įstatymai bei reglamentai susiję su DI veikla
Jungtinės karalystės	BDAR
	Duomenų apsaugos įstatymas (2018 m.)

*6 lentelė **„Jungtinės karalystės įstatymai bei reglamentai susiję su DI veikla“***

Šalyje norima įgyvendinti ir įkurti daug naujų institucijų bei organizacijų, kurios būtų atsakingos už vieną ar kitą DI stebėsenos, koordinavimo grandį: DI komisija, Duomenų etikos taryba, DI biuras, Duomenų etikos ir inovacijų centras, DI laboratoriją (Roberts, Babuta, Morley, et. al., 2022, p. 2-3; Cath, , Wachter, Mittelstadt, 2018, p. 19). JK taip pat dirba duomenų apsaugos priežiūros pareigūnai, kurie prižiūri ar tinkamai naudojami asmeniniai duomenys. Nors JK Informacijos komisaro tarnyba (ICO) neseniai paskelbė DI audito gaires nurodoma, kad vis dar trūksta priemonių, kaip standartizuotai spręsti DI procesus (Almeida, Shmarko ir Lomas, 2022, p. 5). Šalyje egzistuoja Poveikio duomenų apsaugai vertinimai, kurių metu nustatoma rizika, kylanti tvarkant duomenis pvz.: veido atpažinimo programoms. Taip pat JK veikia neįstatyminės tačiau privalomosios oficialios nacionalinės gairės, kaip policijos veikla turėtų naudoti veido atpažinimo technologijas, kad jos užtikrintų duomenų apsaugą ir žmonių teises (Almeida, Shmarko ir Lomas, 2022, p. 4). Nurodoma jog „tarptautinė humanitarinė teisė išlieka tinkamu teisiniu pagrindu ir sistema vertinant visų ginklų sistemų naudojimą ginkluotuose konfliktuose", šioje dalyje taip pat akcentuoja komunikaciją visuomenei – jog žmonės išliks šių ginklų kontrolės sistemoje (Cath, Wachter, Mittelstadt, 2018, p. 20).

Viename iš šaltinių buvo nurodoma jog teisinės sistemos pagrindų **Estijoje** iš esmės keisti nereikia, o atskiras DI įstatymas yra nereikalingas (Hinton, 2021, p. 23; Kerikmäe ir Pärn-Lee, 2021, p. 7). Šiuo požiūriu Estija labai panaši į JK, nes tokį reguliavimą sieja su laisve inovacijoms. Šalyje buvo teiktos rekomendacijos iš dalies pakeisti daugybę reglamentų, kurie trukdo priimti savaime besimokančias algoritmines sistemas, siūlė vengti perteklinio reglamentavimo ir atlikti būtinus atskirus galiojančių teisės aktų pakeitimus, užuot priėmus naują, atskirą teisės aktą (Tupay et. al., 2021, p. 109). Estijos Vyriausybės vyriausiasis duomenų pareigūnas, aktyviai dalyvauja DI teisės aktų kūrime (e.estonia, 2022), tačiau Estijoje (kol kas) nėra teisės aktų, kuriuose būtų konkrečiai aptariamos DI sistemos, vietoj to yra taikomi bendrieji įstatymai (Tupay et. al., 2021, p. 109). Šalyje yra teisės aktų akcentuojančių skaitmeninės visuomenės reguliavimą (Hinton, 2021, p. 23), taip pat nurodoma jog DI naudojimo procesus liečia kiti teisės šaltiniai: Kibernetinio saugumo įstatymas, Civilinio proceso kodeksas, Teisėsaugos įstatymas, Valstybės atsakomybės įstatymas (Tupay et. al., 2021, p. 109). Duomenų privatumą Estijoje pirmiausia reglamentuoja Asmens duomenų apsaugos įstatymas (EPDPA), kuris padeda įgyvendinti BDAR (IndiaAI, 2020) (*žr. 7 lentelę*).

Šalis	Įstatymai bei reglamentai susiję su DI veikla
Estija	BDAR
	Asmens duomenų apsaugos įstatymas (EPDPA)
	Kibernetinio saugumo įstatymas
	Civilinio proceso kodeksas
	Teisėsaugos įstatymas
	Valstybės atsakomybės įstatymas

*7 lentelė **„Estijos įstatymai bei reglamentai susiję su DI veikla“***

Estija nurodo jog BDAR įstatymas turi išimčių, pvz. jis netaikomas, kai duomenys tvarkomi dėl nusikalstamų veikų prevencijos, baudžiamojo persekiojimo, atliekamų tyrimų. (Tupay et. al., 2021, p. 100). Estija taip pat priėmė naują Asmens duomenų apsaugos įstatymo redakciją, jog įstatymai atitiktų ES teisę. Perkeliant teisėsaugos direktyvą į nacionalinę teisę, buvo nuspręsta, kad grėsmių visuomenės saugumui prevencija pateks ne į šios direktyvos, o į BDAR taikymo sritį, taip taikant griežtesnės taisyklės (Tupay et. al., 2021, p. 108). Toks poelgis atskleidžia šalies perspektyvą – norą silpninti DI reguliavimą, bet taikyti griežtesnį rizikų ir žalų valdymą.

Vokietijoje (Bavarijoje ir Hesene) yra įsteigtos skaitmeninimo ministerijos subnacionaliniu lygmeniu, o šios institucijos skelbia įvairius dokumentus dėl DI (Hinton, 2021, p. 4), minima jog tai parodo politikos formuotojų „arčiau visuomenės“ kryptį (galime sugretinti su anksčiau minėta į žmogų

orientuota DI pozicija, nors to šalis tiesiogiai neįvardina). Vokietijos duomenų apsaugos standartai yra itin aukšti (Köstler ir Ossewaarde, 2022, p. 5), tačiau apie juos niekur nėra išsiplečiama kalbant apie DI naudojimą. Nurodoma, kad DI turėtų būti siaurai reguliuojamas BDAR, kadangi jis apima, asmens duomenis, privatumo užtikrinimo, automatizuoto sprendimų priėmimo ir profiliavimo apribojimus, kurie liečia DI technologijas.

Šalis	Įstatymai bei reglamentai susiję su DI veikla
Vokietija	Vokietijos federalinės informacijos saugumo tarnybos įstatymas
	BDAR

*8 lentelė **„Vokietijos įstatymai bei reglamentai susiję su DI veikla“***

Dėl šios priežasties nebūtina kurti naujų įstatymų, nes tai taptų pertekliniu DI reguliavimu, kuris neskatintų inovacijų (AICGS, 2022) – šio požiūrio kartu laikosi Estija bei JK. Vokietijoje kuriamas nacionalinis DI standartų nustatymo procesas, kuriame aptariami tokie aspektai kaip šališkumas, patikimumas, teisingumas bei audito ir sertifikavimo galimybės (Simbeck, 2022). Sertifikavimo pagalbą taip pat gali užtikrinti Vokietijos informacijos saugumo tarnybos IT bazinės apsaugos katalogai, kuriuose galima pasitikrinti ar įmonės ėmėsi visų reikalingų veiksmų susijusių su DI naudojimu (Wischmeyer ir Rademacher, 2019, p. 22), tačiau abejotina (bei niekur nepažymėta) ar ši sistema gali būti taikoma ir teisėsaugos institucijoms. Vokietijos federalinės informacijos saugumo tarnybos įstatymas siekia užkirsti kelią informacinių technologijų sistemų prieinamumo, vientisumo, autentiškumo ir konfidencialumo trikdžiams, kas iš esmės tik netiesiogiai liečia DI veiklą. Šalies vyriausybė taip pat pasisakė prieš visiško veido atpažinimo ir DI technologijų naudojimo viešose erdvėse (AICGS, 2022), tai gali rodyti norą apsaugoti asmenų privatumą arba nevisišką užtikrintumą šiomis technologijomis. Vokietijos Bundestagas įsteigė DI komisiją "Enquete", kuri taip pat planuoja spręsti etinius klausimus (Wischmeyer ir Rademacher, 2019, p. 24).

Apibendrinant, matosi aiškus dėsningumas – visos šalys vienu ar kitu požiūriu mini BDAR įstatymo svarbą jų teisėja kalbant apie DI sistemų naudojimą. Išskirtinai Belgija, Prancūzija ir Estija nurodo BDAR įstatymo ribas bei išimtis. Bendras šalių panašumas – tai jog nei viena neturi tiesioginio nacionalinio DI įstatymo, o jo veiklą reguliuoja per kitus reglamentus bei teisės aktus. Kai kurios šalys, pvz.: JK bei Estija pasižymi plataus pobūdžio komunikacija apie taikomus įstatymus bei esamas atskiras valstybės grandis, kurios užsiima DI stebėsena bei koordinavimu. Estija, JK ir Vokietija išreiškia bendrą požiūrį – DI veikla neturėtų būti pertekliniai reguliuojama ir svarbu suteikti laisvę inovacijoms. Viešai prieinamoje informacijoje Vokietija, šia tema išsiskiria, kaip šalis labiausiai

akcentuojanti ir susitapatinanti su ES reglamentais, projektais bei nurodo tik kelias neįstatymines valstybės grandis, kurios gali reguliuoti DI, o tai kelia klausimą ar jų nėra, ar šalis apie jas neskelbia?

2.5. Viešai prieinama TPŠ informacija apie naudojamas DI sistemas teisėsaugoje

Šioje darbo dalyje atskleidžiamos šalių teisėsaugos sistemoje naudojamos DI technologijos, kurios yra pateikiamos viešai prieinamoje informacijoje. Bendras šalių vaizdas nurodo jog DI programos daugiausiai naudojamos lengviems teisiniams klausimams spręsti bei dokumentams apdoroti, taip pat gynybos sektoriuje, vaizdo stebėjimo ir vagysčių-įsilaužimų prognostikoje. Rečiau taikomos specifiškose srityse pvz.: gaujų aptikimo, auditavimo, efektyviausios pagalbos asmeniui nutraukti nusikalstamą veiką pateikimas. 3-iame šio darbo priede taip pat yra pateikta detalesnė informacija apie šalių naudojamas sistemas, jų paskirtį bei informacijos šaltinius. Toliau aptariama 9 lentelėje pateikta informacija:

Estijoje daugiausia informacijos randama apie naudojamus bepiločius orlaivius bei karinės paskirties priemones. Šalyje yra naudojama teksto analizės bei teisinius klausimus padedanti spręsti sistema. Pastebėta jog nėra jokios komunikacijos apie naudojamas prognostines arba veido atpažinimo sistemas. Svarbu paminėti ir atsiradusį disonansą, keliuose ne tik publicistiniuose (Forte, The Lawyer's Daily, Wired), tačiau ir moksliniuose leidiniuose (Campbell, 2020, p. 345; Walker-Osborn ir Chan, 2017, p. 11) buvo nurodomas Estijos planas ar netgi įsibėgėjęs procesas įvesti DI teisėją, kuris būtų nepriklausomas ir galėtų priimti sprendimus dėl ieškinių iki 7 000 eur. Tačiau Estijos teisingumo ministerija 2022 m. vasario mėnesį išleido paaiškinimą jog šiuo metu neturi DI paremtų sistemų, o vieninteliame transkripcijos projekte yra naudojamas MM. Būtent toks komunikacijos disonansas kelia susirūpinimą ties pasiekiama informacija apie šalių naudojamas DI sistemas, tai gali klaidinti bei sudaryti visai kitokį šalies įvaizdį.

Vokietija gan plačiai atskleidžia naudojamas sistemas vagysčių ir įsilaužimų aptikimo srityse, prognostinės policijos veikloje. Šalis taip pat nurodo jog naudoja programas siekiant aptikti terorizmo rizikas. Taip pat nurodoma naudojama vaizdo apdorojimo programa. Iš teisinės – administracinės pusės pavyko atrasti naudojamą sistemą padedančią atlikti tyrimus. Lyginant su Estija, Vokietija nesiplečia ir nenurodo naudojamų DI sistemų karinėje – gynybos srityje.

Prancūzija išsiskiria viešai prieinama komunikacija apie plataus pobūdžio DI naudojimą. Nurodoma keletą analizės bei paieškos sistemų, kurios palengvina darbą teisės srityje. Nurodomi

masinio stebėjimo, elgesio stebėjimo kameromis bei dronais – būdai, kurie siejami ne tik su nusikalstamo elgesio aptikimu, bet ir terorizmo rizikų nustatymu.

DI technologijos:	JK	Belgija	Prancūzija	Estija	Vokietija
Grėsmės vertinimo sistema *(skubios pagalbos centro darbo optimizavimas pateikiant rizikos dydžio vertinimą)*				+	
Optimaliausių intervencijų asmeniui nustatymas *(asmeniui sudaromas efektyviausia paslaugų programa padėsianti nutraukti nusikalstamą veiką)*	+				
Asmenų pakartotinio nusikalstamumo rizikos grupių skirstymas	+ +				+
Žvalgybos priemonė gaujų smurto atvejais	+				
Karinės informacijos analizė *(sistema galinti analizuoti didžiulius kiekius duomenų, gaunamų iš karinės įrangos)*			+		
Gynybos sektorius *(įvairios paskirties karinės kilmės ginklai)*		+	+	+ + + + + + +	
Teksto analizės paslaugas *(duomenų paieškos, kodavimo, kategorizavimo funkcijos)*				+	
Transkribavimo teisminiame procese paslaugos				+	
Palengvina atlikti įsilaužimų ir vagysčių tyrimus					+
Duomenų bazė *(atliekant teisminius ir administracinius tyrimus)*			+		
Dokumentų patikra auditavimo srityje			+		
Vagysčių ir įsilaužimų prognostika		+ + +	+		+ + +
Patruliavimo maršrutų sudarymas		+			+
Teisinių klausimų sprendimas *(paruošia reikiamus dokumentus bei teikia reikalingą informaciją asmeniui taip lengvindamas administracinį teisininkų darbą)*	+	+	+ +	+	
Teisinių bylų bei dokumentų analizė	+	+ +	+ +		
Terorizmo rizikos bei išpuolių nustatymas			+		+ +
Vaizdo stebėjimo sistema *(netinkamo arba įtariamo elgesio aptikimas bei fiksavimas perduodant informaciją teisėsaugai)*		+	+ +		+
Dronai *(naudojami gynybos srityje bei vaizdo stebėjimui)*	+		+		+
Finansinių operacijų stebėjimas	+		+		
KET pažeidimų nustatymas	+		+		

*9 lentelė **„Teisėsaugoje naudojamo dirbtinio intelekto sritys“.** Lentelėje nurodytos viešai prieinamoje informacijoje randamos šalių naudojamos DI sistemos teisėsaugoje. Kiekvienas pliusas reprezentuoja atskirą sistemą-technologiją.*

JK iš internete prieinamos medžiagos atrodo daugiausiai dėmesio skirianti prognostikai bei asmenų įvertinimui skirstant į rizikos grupes. Šalyje naudojamos analizę palengvinančios sistemos teisės srityje. Vienoje iš publikacijų buvo aptiktas neleistinas veidų atpažinimo atvejis, kuris tęsėsi 2 metus, tai tik įrodo šių sistemų panaudojimo grėsmes ir kelia anksčiau minėtus etinius klausimus. Taip pat, kaip ir Vokietija, nenurodo karinės – gynybos paskirties priemonių.

Panaši situacija su veido atpažinimo sistema pasitaikė ir Belgijoje, procesui sustabdyti įsikišo ne tik teismas, tačiau ir duomenų apsaugos tarnyba. Laisvai prieinamoje informacijoje matoma jog Belgijoje naudojamos tiek prognostinės tiek teisminio proceso, dokumentų analizei skirtos sistemos. Prieinama informacija ir apie gynybos srityje naudojamas priemones.

Tvirtai teigti, kad šalys naudoja skirtingai (arba dėsningai) panašaus pobūdžio sistemas – neobjektyvu, kadangi skirtumas gali būti pačioje komunikacijoje, kai viena šalis – Prancūzija, ganėtinai išsamiai nurodo naudojamas sistemas, o pvz.: Estija turi itin mažai viešai prieinamos informacijos šia tema. Tačiau vien iš analizuotų duomenų, dėsningumas matosi vagysčių-įsilaužimų prognozės sistemų naudojime bei greitesnei duomenų-dokumentų analizei pritaikytos technologijos. Iš esmės didžioji dauguma nurodomų technologijų orientuotos į duomenų analizę ir tik mažoji dalis į fizinę kontrolę (pvz.: vaizdo stebėjimo priemones). Toks atradimas suponuoja jog naudojamos sistemos pačios iš savęs yra gan mažos rizikos, o tinkamai naudojant ir pritaikant gautą informaciją galima gauti daug naudos taip gerinant teisėsaugos našumą.

Apibendrinant, DI technologijos, tokios kaip įsilaužimų prognozės, optimalių patruliavimo maršrutų sudarymas leidžia teisėsaugos sistemai efektyviai išnaudoti turimus resursus bei pagerinti savo veiklos rezultatus. Verta pastebėti jog viešai prieinamoje informacijoje nurodomas tik siaurasis DI, jis naudojamas tam tikros specifinės srities palengvinimui, o tai tik patvirtina teorinėje dalyje išskirtus DI limitus teisėsaugoje. Analizuojant tik straipsniuose ar publikacijose esančią informaciją negalima teigti jog konkreti šalis aktyviau naudoja DI požymių turinčias sistemas už kitą, nes tai gali reikšti tik aktyvesnę informacijos skaidą šia tema. Vertinant tik nagrinėjamos literatūros kontekste, Vokietija bei Prancūzija pateikia daugiausiai naudojamų sistemų, kurios iš esmės skiriasi. Vokietija daugiau nurodo priemonių, kurios padeda prognozuoti arba numatyti nusikaltimo rizikas, o Prancūzija orientuojasi į teksto analizės bei kitų administracinių darbų palengvinimą bei vaizdo stebėjimą. Taip pat verta atkreipti dėmesį jog teisėsaugoje naudojamų priemonių atskleidimas gali neigiamai paveikti

darbo efektyvumą bei sukelti pavojų šalies saugumui ir dėl šios priežasties šalys gali vengti viešai skelbti informaciją šia tema.

2.6 Rezultatų apibendrinimas ir diskusija

Visos šalys įvardydamos DI principus paminėjo saugumo, patikimumo, skaidrumo, duomenų apsaugos, nediskriminavimo aspektus, o tai atskleidžia jog visos šalys mini pagrindinius principus, kurie saugo jautriausias sritis, kurios visuomenėje susilaukia daug dėmesio. Šalys išsiskiria pavieniais principais, tokiais kaip bendradarbiavimas, komandų įvairovė sistemų kūrimo procese, duomenų prieinamumas, kurie iš esmės nesusilaukia didelio dėmesio visuomenėje, tačiau mokslinėje literatūroje šie principai yra itin svarbūs visame technologijų gyvavimo cikle.

Lyginant tyrime aprašytą informaciją apie šalių patirtį DI kontekste su teorine dalimi, galima įvardinti daugelį vietų, kuriose šalys galėtų tobulėti, pvz.: aprašant DI principus, nurodant gilesnes įžvalgas apie naudos ir žalos galimybes, taip suteikiant visuomenei platesnį šių sistemų suvokimą. Kolkas vaizdas DI strategijose bei kitoje viešai prieinamoje informacijoje, šiame kontekste, išlieka labai bendras ir ganėtinai paviršutinis. Išskyrus JK, tyrime nagrinėjamos šalys nesuteikė daug dėmesio galimų DI grėsmių nurodymui – nebuvo galima išskirti bendros žalos, o tai gali būti dėl nenoro sukelti baimės visuomenėje. Kai kurios šalys, tokios kaip JK ir Vokietija, minėdamos galimas rizikas, kartu stengėsi nurodyti jų valdymo būdus.

Nors kai kurios šalys pozityviai išsiskiria vienose vietose (pvz. Vokietija aprašant naudos galimybes, Prancūzija nurodydama naudojamų sistemų gausą), tos pačios šalys negatyviai pasižymi kitose srityse (Prancūzija nenurodo jokių DI grėsmių, Vokietija turi mažai prieinamos informacijos apie apsaugos būdus bei taikomus įstatymus DI technologijoms). Tuo tarpu Estija išsiskiria, kaip šalis kuri mažiausiai pasižymi turima informacija apie DI teisėsaugoje, nors analizuojamoje literatūroje ši šalis nurodoma, kaip siekianti automatizuoti valstybinius procesus bei turinti labai aktyvią veiklą duomenų rinkimo ir DI sferoje. Tai kelia prielaidą jog šalis nėra suinteresuota skelbti šios informacijos visuomenei.

Į žmogų orientuoto DI kryptis išlieka menkai akcentuojama – trys šalys (Estija, Belgija ir Vokietija) apie šią kryptį tik užsiminė. Tai nurodo tam tikrą šalių nesuinteresuotumą arba žinių trukumą apie šios krypties naudojimą taikant DI technologijas. Lyginant su moksline literatūra, tai ne tik daug dėmesio sulaukianti tema tačiau ir labai skatintina DI taikymo kryptis, kuri mokslininkų

nuomone, teiktų daug naudos ne tik visuomenei bet ir valstybei (vertinant tai jog visuomenė labiau pasitikinti šiomis technologijomis leis valstybei aktyviau tobulėti šioje srityje).

Daugelis šalių yra linkusios nekurti perteklinio reguliavimo, o kaip tik propaguoti laisvą duomenų judėjimą ir laisvę inovacijoms. Atsižvelgiant į mokslinę literatūrą tai nėra negatyvus požiūris, tačiau tam, kad šios technologijos veiktų visuomenės naudai, tampa būtina sukurti atitinkamus apsaugos mechanizmus, jų veiklai reguliuoti. Estija, JK bei Vokietija pasižymėjo, kaip šalys, kurios siekia neapsunkinti DI įgyvendinimo procesų įstatyminiu būdu bei suteikti laisvę inovacijoms. Tačiau Vokietija (kartu ir Prancūzija) nenurodė pakankamai DI technologijų apsaugos grandžių, o tai sukelia riziką žaloms įvykti.

Bendras šalių vaizdas nurodo jog DI programos daugiausiai naudojamos lengviems teisiniams klausimams spręsti bei dokumentams apdoroti, taip pat gynybos sektoriuje, vaizdo stebėjimo ir vagysčių-įsilaužimų prognostikoje. Rečiau taikomos specifiškose srityse pvz.: gaujų aptikimo, auditavimo, efektyviausios pagalbos asmeniui nutraukti nusikalstamą veiką rekomendacijoms. Vokietija bei Prancūzija išsiskyrė nurodomų technologijų gausa, tačiau tarp šalių, jų paskirtis skiriasi: Vokietija daugiau nurodo prognostines arba nusikaltimo rizikas nustatančias sistemas, o Prancūzija – teksto analizės bei kitų administracinių darbų palengvinimo bei vaizdo stebėjimo technologijas. Šių ar kitų DI sistemų naudojimas priklauso ir nuo teisėsaugai skiriamų resursų, todėl DI potencialo neišnaudojimą dalinai galima sieti su šia priežastimi.

Iš viešai prieinamos informacijos apie naudojamas DI technologijas teisėsaugoje galime daryti prielaidas jog tai dar labai nauja sritis, kadangi naudojamos sistemos dažnu atveju skirtos administracinėms veikloms palengvinti, rečiau specifinių situacijų prognozavimui. Šios sistemos iš esmės duoda daug naudos didinant teisėsaugos našumą ir teikia mažą riziką žalai įvykti.

Išvados

Dažnu atveju DI yra sunkiai apibrėžiamas bei atskiriamas nuo kitų pogrupių, kadangi jis apima tiek MM tiek GM sistemas. Mokslinėje literatūroje nėra nuoseklumo DI sistemų apibrėžime, tačiau išsiskiria pasikartojanti savybė – žmogaus intelekto bruožų ir galimybių mimikavimas. Mokslinėje literatūroje pasikartojantys principai išlieka: duomenų apsauga, atsakomybė ir atskaitomybė, skaidrumas, audito galimybė bei suinteresuotųjų šalių įtraukimas į DI procesus. Principams būdinga: sąsaja tarpusavyje – įgyvendinant vieną privalu įgyvendinti ir kitą, dažnai principuose atsiskleidžia DI technologijų nauda. Teorinėje dalyje, dažniausiai minima sistemų žala teisėsaugoje yra galimas duomenų šališkumas bei duomenų apsaugos neužtikrinimas. Tačiau žala gali atsirasti ir dėl darbuotojų, kurie neturi pakankamai žinių, jog galėtų tinkamai naudotis technologijomis. Dažniausiai minima DI nauda, mokslinėje literatūroje, yra galimybė pagreitinti procesus bei veiksmingiau išnaudoti turimus teisėsaugos resursus finansine, laiko, bei darbuotojų prasme.

Tiriamos šalys, nurodydamos tik jautriausias sritis liečiančius principus, neskiria daugiau dėmesio principams, kurie yra akcentuojami mokslinėje literatūroje. Strategijose šalys dažai blankiai aprašo DI technologijų naudas ir grėsmes, o tai gali sudaryti iškreiptą DI potencialą visuomenei. Į žmogų orientuoto DI kryptį mini tik trys šalys: Estija, Belgija ir Vokietija. Tai rodo šalių nesuinteresuotumą arba žinių trukumą apie šios krypties galimybes taikant DI teisėsaugoje. Nei viena šalis neturi tiesioginio nacionalinio DI įstatymo, o jo veiklą reguliuoja per kitus teisės aktus arba atskiras valstybės grandis. Estija, JK bei Vokietija atsisako perteklinio reglamentavimo ir pabrėžia laisvę inovacijoms, tačiau tokiu atveju DI technologijoms turi būti sukurtos kitos priemonės, kurios galėtų prižiūrėti ir koordinuoti jo veiklą – viešai prieinamoje informacijoje, Vokietijos ir Prancūzijos kontekste, šių priemonių stinga. Didžioji dauguma nurodomų technologijų orientuotos į duomenų analizę ir tik labai maža dalis į fizinę kontrolę, o tai nurodo mažesnį rizikos ir didesnį naudos potencialą jeigu sistemos bus naudojamos tinkamai. Sistemų naudojimo dėsningumas matosi vagysčių-įsilaužimų aptikimui bei dokumentų ar duomenų analizei atlikti, tai gana žemos rizikos sistemos, kurios gali optimizuoti policijos veiklą. Tačiau neaktyvus šių technologijų taikymas šalyse dalinai gali būti siejamas su lėšų joms trūkumu.

Tyrimo trūkumas – analizuota tik viešai prieinama informacija, o tai gali priklausyti nuo aktyvesnės informacijos sklaidos šia tematika šalyje. Kadangi tai jautri informacija, dėl visuomenės ir valstybės saugumo, teisėsauga ne visuomet gali viešinti, kokias DI priemones taikomos jų šalyje, todėl šios informacijos prieinamumas yra limituotas. Tyrimo privalumai – parodo Europos geografinėje

zonoje esančia situaciją apie DI naudojimą teisėsaugoje, požiūrį į jo taikymą, bei nurodo, kuriose vietose šalys turėtų įdėti daugiau pastangų tobulinant DI strategijas ir pristatant šias technologijas visuomenei. Kituose tyrinėjimuose, aktualu analizuoti informaciją, kuri nėra tik viešai prieinama. Ateityje, pravartu apklausti teisėsaugos sistemoje dirbančius asmenis ir atlikti gilesnį tyrimą šia tematika, pasitelkiant interviu ar anketų pagalbą.

Literatūra

Mokslinė literatūra:

1. Almeida, D., Shmarko, K. ir Lomas, E. (2022) ‘The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks’, *AI and Ethics*, 2(3), p. 377–387.
2. Amilevičius, D. (2017) ‘Dirbtinis intelektas ir besiformuojančių technologijų etika’, *Naujasis židinys - Aidai*, 4, p. 19–24.
3. Aoki, N. (2021) ‘The importance of the assurance that “humans are still in the decision loop” for public trust in artificial intelligence: Evidence from an online experiment’, *Computers in Human Behavior*, 114, p. 106-572.
4. 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.
5. Babuta, A. ir Oswald, M. (2019) ‘Data Analytics and Algorithmic Bias in Policing’, *Royal united services institute for defence and security studies*.
6. Barysė, D. ir Sarel, R. (2022) ‘Algorithms in the Court: Does it Matter Which Part of the Judicial Decision-Making is Automated?’, *Artificial Intelligence and Law*.
7. Berryhill, J. et al. (2019) ‘Hello, World: Artificial Intelligence and its use in the Public Sector’, *OECD Observatory of Public Sector Innovation (OPSI)*, 36.
8. Boahemaa, F. J. (2019) ‘The impact of artificial intelligence on justice systems, Trento BioLaw Selected Student Papers’.
9. Bouman J., (2021) ‘Preventing corruption of civil servants in France, Romania and Netherlands: a comparative study of law and policy’ *University Utrecht*.
10. Campbell, R. W. (2020) ‘Artificial Intelligence in the Courtroom : the Delivery of Justice in the Age of Machine Learning’, *Colorado Technology Law Journal*, 18(2), p. 323–350.
11. Casey, D., Burrell, P. ir Sumner, N. (2019) ‘Decision Support Systems in Policing.’, *European Law Enforcement Research Bulletin*, 4, p. 97.
12. Cath, C., Wachter, S., Mittelstadt, B. et al. (2018) ‘Artificial Intelligence and the “Good Society”: the US, EU, and UK approach.’, *Sci Eng Ethics*, 24, p. 505–528.
13. Christakis T. ir Trotry A. (2020) ‘French White Paper on Internal Security Makes Several Proposals for the Use of Facial Recognition in France’, *AI-Regulation*.

14. Ciston, S. (2019) ‘Intersectional artificial intelligence is essential: Polyvocal, multimodal, experimental methods to save AI’, *Journal of Science and Technology of the Arts*, 11(2), p. 3–8.
15. Degeling, M. ir Berendt, B. (2018) ‘What is wrong about Robocops as consultants? A technology-centric critique of predictive policing’, *AI and Society*, 33(3), p. 347–356.
16. Egbert, S. (2018) ‘About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany’, *European Journal for Security Research*, 3(2), p. 95–114.
17. Egbert, S. (2019) ‘Predictive policing and the platformization of police work’, *Surveillance and Society*, 17(1–2), p. 83–88.
18. Egbert, S. ir Krasmann, S. (2020) ‘Predictive policing: not yet, but soon preemptive?’, *Policing and Society*, 30(8), p. 905–919.
19. Gerstner, D. (2018) ‘Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany’, *European Journal for Security Research*, 3(2), p. 115–138.
20. Hinton C. P. (2021) ‘The State of Ethical AI in Practice: A Multiple Case Study of Estonian Public Service Organizations’, *Miunsterio universitetas*.
21. Ibarra, G., Douglas, D. M. ir Tharmarajah, M. (2020) ‘Machine Learning and Responsibility in Criminal Investigation’, *Australia’s National Science Agency*.
22. 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.
23. Jobin, A., Ienca, M. ir Vayena, E. (2019) ‘The global landscape of AI ethics guidelines’, *Nature Machine Intelligence*, 1(9), p. 389–399.
24. Joh, E. E. (2018) ‘Artificial Intelligence and Policing: First Questions’, *Seattle University Law Review*, 41(4), p. 1139–1144.
25. Johansson, R. (2007) ‘On case study methodology’, *Open House International*, 32(3), p. 48–54.
26. Karppi, T. (2018) “The Computer Said So”: On the Ethics, Effectiveness, and Cultural Techniques of Predictive Policing’, *Social Media and Society*, 4(2).
27. Kerikmäe, T. ir Pärn-Lee, E. (2021) ‘Legal dilemmas of Estonian artificial intelligence strategy: in between of e-society and global race’, *AI and Society*, 36(2), p. 561–572.

28. Köstler, L. ir Ossewaarde, R. (2022) ‘The making of AI society: AI futures frames in German political and media discourses’, *AI and Society*, 37(1), p. 249–263.
29. Land, M. K. ir Aronson, J. D. (2020) ‘Human rights and technology: New challenges for justice and accountability’, *Annual Review of Law and Social Science*, 16, p. 223–240.
30. Leslie, D. (2019) ‘Understanding artificial intelligence ethics and safety systems in the public sector’, *The Alan Turing Institute*.
31. Lyuben, A. et al. (2021) Predictive Policing in the Belgian Police Service.
32. Meijer, A. ir Wessels, M. (2019) ‘Predictive Policing: Review of Benefits and Drawbacks’, *International Journal of Public Administration*, 42(12), p. 1031–1039.
33. Moses, L. B. ir Chan, J. (2018) ‘Algorithmic prediction in policing: assumptions, evaluation, and accountability’, *Policing and Society*, 28(7), p. 806–822.
34. Murauskas, D. (2020) ‘Dirbtinis intelektas priimant teismo sprendimą – algoritmų klasifikavimas remiantis teisinio kvalifikavimo stadijomis’, 115, p. 55–69.
35. Negri S. (2021) ‘innovations in the legal services supported by the use of visual law: the reality in Finland and Belgium’, p. 1-13.
36. Oswald, M. et al. (2018) ‘Algorithmic risk assessment policing models: Lessons from the Durham HART model and “experimental” proportionality’, *Information and Communications Technology Law*, 27(2), p. 223–250.
37. Petkeviciute-Barysiene, D. (2021). ‘Human-automation interaction in law: mapping legal dessicions, cognitive processes, and automation levels’, p. 340-344.
38. Rashid, Y. et al. (2019) ‘Case Study Method: A Step-by-Step Guide for Business Researchers’, *International Journal of Qualitative Methods*, 18, p. 1–13.
39. Re, R. . ir Niederman, S. A. (2019) ‘Developing Artificially Intelligent Justice’, *Stanford Technology Law Review*, 242(22), p. 242–289.
40. Roberts, H., et al. (2022) ‘Artificial Intelligence Regulation in the United Kingdom: A Path to Global Leadership?’, p. 1–11.
41. Robinson N., Hardy A. ir Ertan A., (2021) ‘Estonia: A Curious and Cautious Approach to Artificial Intelligence and National Security’, Routledge Companion to Artificial *Intelligence and National Security Policy*.
42. Sampaio, E. A., Seixas, J. J., Gomes P. J. (2019) ‘Artificial intelligence and the judicial ruling”, Bulgaria.

43. Sharma, Z. et al. (2019) ‘The impact of artificial intelligence on healthcare’, Indian Journal of *Public Health Research and Development*, 10(8), p. 189–194.
44. Sultan, A. S. et al. (2020) ‘The use of artificial intelligence, machine learning and deep learning in oncologic histopathology’, *Journal of Oral Pathology and Medicine*, 49(9), p. 849–856.
45. Suresh H. ir Guttag J. (2021) ‘A Framework for Understanding Sources of Harm throughout the Machine Learning Life Cycle’, *ACM International Conference Proceeding Series*.
46. Tellis W. (1997) ‘Application of a Case Study Methodology’, *The Qualitative Report*, 3(3), p. 1–19.
47. Tupay P. K. et al. (2021) ‘Is European Data Protection Toxic for Innovative AI? An Estonian Perspective’, *Juridica International*, 30, p. 99–110.
48. Utka, A. (2021) ‘Du interviu dirbtinio intelekto tema’, *Darbai ir dienos*, 76, p. 121–130.
49. Vrontis, D. et al. (2022) ‘Artificial intelligence, robotics, advanced technologies and human resource management: a systematic review’, *International Journal of Human Resource Management*, 33(6), p. 1237–1266.
50. Walker-Osborn, C. ir Chan, C. (2017) ‘Artificial intelligence and the law’, *Itnow*, 59(1), p. 36–37.
51. Wirtz, B. W., Weyerer, J. C. ir Geyer, C. (2019) ‘Artificial Intelligence and the Public Sector—Applications and Challenges’, *International Journal of Public Administration*, 42(7), p. 596–615.
52. Wischmeyer T. ir Rademacher T., (2020) ‘Regulating Artificial Intelligence’, 1(1), p. 307-321.
53. Završnik, A. (2021) ‘Algorithmic justice: Algorithms and big data in criminal justice settings’, *European Journal of Criminology*, 18(5), p. 623–642.

Tarptautinių organizacijų ar vyriausybių leidiniai:

54. Dolibeau, L. ir Georganta P., (2021) ‘France International Bar Association‘, *IBA Alternative and New Law Business Structures Committee*. Internetinė prieiga: https://www.ibanet.org/MediaHandler?id=1db4c268-b477-48d6-b9fc-d8aaf8e38b80

55. Estijos respublikos vyriausybė (2019) ‘Report of Estonia’s AI Taskforce’. Internetinė prieiga: https://www.kratid.ee/in-english

56. Europos komisija (2020) ‘White Paper on Artificial Intelligence: a European approach to excellence and trust’. Internetinė prieiga: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en

57. Europos parlamentas (2020) ‘Artificial Intelligence and Law Enforcement Impact on Fundamental Rights’.

58. Europos skaitmeninės teisės (2020) ‘Use cases : Impermissible AI and fundamental rights breaches’

59. 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.

60. Europos taryba (2021) ‘EU in the global Artificial Intelligence landscape’. Internetinė prieiga: https://publications.jrc.ec.europa.eu/repository/handle/JRC125613.

61. 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.

62. Europos veiksmingo teisingumo komisija (CEPEJ) (2018) European ethical charter on the use of Artificial Intelligence in judicial systems and their environment.

63. EY Law, (2021) ‚Belgium embraces Artificial Intelligence (AI) for legal document review‘. Internetinė prieiga: https://www.eylaw.be/2019/10/31/ey-law-belgium-embraces-artificial-intelligence-ai-for-legal-document-review/

64. Jungtinės karalystės vyriausybė (2021) ‘National AI Strategy’.

65. Nacionalinė informacijos ir laisvės komisija (CNIL)(2019) ‘Facial Recognition for a Debate Living’. Internetinė prieiga: https://www.cnil.fr/en/facial-recognition-debate-living-challenges

66. Prancūzijos vyriausybė (2021) ‘AI training in higher education’. Internetinė prieiga: (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/talents-et-competences/la-formation-ia-dans-l-enseignement-superieur)

67. Prancūzijos vyriausybė (2021a) ‘Artificial intelligence at the service of companies’. Internetinė prieiga: (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/l-intelligence-artificielle-au-service-des-entreprises)

68. Prancūzijos vyriausybė (2021b) ‘Educate on artificial intelligence’. Internetinė prieiga: https://www.intelligence-artificielle.gouv.fr/fr/thematiques/talents-et-competences/eduquer-l-intelligence-artificielle

69. Prancūzijos vyriausybė (2021c) ‘Ethics of artificial intelligence’. Internetinė prieiga: https://www.intelligence-artificielle.gouv.fr/fr/thematiques/ethique-de-l-intelligence-artificielle

70. Prancūzijos vyriausybė (2021d) ‘Public transformation and data policy’. Internetinė prieiga: https://www.intelligence-artificielle.gouv.fr/fr/thematiques/transformation-publique/transformation-publique-et-politique-de-la-donnee

71. Prancūzijos vyriausybė (2021e) ‘The national strategy for AI’. Internetinė prieiga: (https://www.intelligence-artificielle.gouv.fr/fr/strategie-nationale/la-strategie-nationale-pour-l-ia)

72. UNESCO (2021) The Ethics of Artificial Intelligence.

73. UNESCO (2021a) ‘UNESCO member states adopt the first ever global agreement on the Ethics of Artificial Intelligence’

74. UNICRI ir INTERPOL (2020) ‘Towards Responsible AI innovation. Second INTERPOL - UNICRI report on artificial intelligence for law enforcement’.

75. United nations (2021) ‘193 countries adopt the first global agreement on the Ethics of Artificial Intelligence. UN News’, *Culture and education*. Internetinė prieiga: https://news.un.org/en/story/2021/11/1106612.

76. Vokietijos federalinė vyriausybė (2020) ‘Artificial Intelligence Strategy of Germany Federal Government’.

Internetinės publikacijos:

77. ‘AI-4Belgium’ (2021), p. 1–29. Internetinė prieiga: https://www.ai4belgium.be/

78. Automating society 2019 – France. Internetinė prieiga: https://algorithmwatch.org/en/automating-society-2019/france

79. Automating society 2019 – Germany. Internetinė prieiga: https://algorithmwatch.org/en/automating-society-2019/germany

80. Belgian army to buy RQ-20 Puma and RQ-21 Integrator drones. Internetinė prieiga: https://www.armyrecognition.com/defense_news_december_2020_global_security_army_industry/belgian_army_to_buy_rq-20_puma_and_rq-21_integrator_drones.html

81. Can AI Be a Fair Judge in Court? Estonia Thinks So. Internetinė prieiga: https://www.wired.com/story/can-ai-be-fair-judge-court-estonia-thinks-so/

82. Deloitte (2020) ‘Urban Future With a Purpose’. Internetinė prieiga: https://www2.deloitte.com/global/en/pages/public-sector/articles/urban-future-with-a-purpose/15-minute-city.html

83. Doctrine – sistema. Internetinė prieiga: https://www.appengine.ai/company/doctrine

84. Estonia does not develop AI Judge. Internetinė prieiga: https://www.just.ee/en/news/estonia-does-not-develop-ai-judge

85. France approves final phase of Artemis big-data processing platform. Internetinė prieiga: https://www.defensenews.com/global/europe/2022/07/11/france-approves-final-phase-of-artemis-big-data-processing-platform/

86. France: Artificial Intelligence Comparative Guide. Internetinė prieiga: https://www.mondaq.com/france/technology/1059760/artificial-intelligence-comparative-guide

87. French DGA selects Athea for phase three of Artemis.IA project. Internetinė prieiga: https://www.army-technology.com/news/athea-create-operational-artemis-ia-platform/

88. Gangs violence matrix – sistema. Internetinė prieiga: https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/

89. Hadron – sistema. Internetinė prieiga: https://mecatron.rma.ac.be/index.php/projects/hadron/

90. Hugo – sistema. Internetinė prieiga: https://www.linkedin.com/company/hugolegalai/?originalSubdomain=ee

91. Istema. Internetinė prieiga: https://www.caselawanalytics.com/

92. Lexis 360 - What is the difference between JurisData analysis and JurisData Analytics? Internetinė prieiga: https://assistance.lexisnexis.fr/hc/fr/articles/360007174272-Lexis-360-Quelle-est-la-diff%C3%A9rence-entre-l-analyse-JurisData-et-JurisData-Analytics-

93. Luminance – sistema. Internetinė prieiga: https://www.luminance.com/

94. Predictice – sistema. Internetinė prieiga: https://predictice.com/fr

95. Ross intelligence sistema. Internetinė prieiga: https://www.rossintelligence.com/features

96. Security News This Week: Hero Chatbot Lawyer Overturns 160,000 Parking Tickets. Internetinė prieiga: https://www.wired.com/2016/07/security-news-week-hero-chatbot-lawyer-overturns-160000-parking-tickets/

97. TEXTA – sistema. Internetinė prieiga: https://www.texta.ee/

Priedai

1 priedas „Moksliniai šaltiniai padarę įtaką šalių pasirinkimui“

Technologiškai pažengusi šalis	Šaltiniai argumentacijai
Estija	– Boahemaa, F. J. (2019) The impact of artificial intelligence on justice systems, Trento BioLaw Selected Student Papers. – Campbell, R. W. (2020) ‘Artificial Intelligence in the Courtroom : the Delivery of Justice in the Age of Machine Learning’, *Colorado Technology Law Journal*, 18(2), p. 323–350. – Europos taryba (2018) ‘Fostering a European approach to Artificial Intelligence’, *e-conversion - Proposal for a Cluster of Excellence*, p. 29–50. – Jamie Berryhill et al. (2019) ‘Hello, World: Artificial Intelligence and its use in the Public Sector’, *OECD Observatory of Public Sector Innovation (OPSI),* (36), p. 1–148. – Europos taryba (2021) ‘EU in the global Artificial Intelligence landscape’
Jungtinės karalystės (JK)	– Oswald, M. et al. (2018) ‘Algorithmic risk assessment policing models: Lessons from the Durham HART model and “experimental” proportionality’, *Information and Communications Technology Law*, 27(2), p. 223–250. – Leslie, D. (2019) ‘Understanding artificial intelligence ethics and safety systems in the public sector’, *The Alan Turing Institute*. – UNICRI ir INTERPOL (2020) ‘Towards Responsible AI innovation. Second INTERPOL - UNICRI report on artificial intelligence for law enforcement’’.
Belgija	– Walker-Osborn, C. and Chan, C. (2017) ‘Artificial intelligence and the law’, *Itnow*, 59(1), p. 36–37 – Lyuben, A. et al. (2021) ‘Predictive Policing in the Belgian Police Service’. – Europos parlamentas (2020) ‘Artificial Intelligence and Law Enforcement Impact on Fundamental Rights’ – Deloitte (2020) ‘Urban Future With a Purpose’. – Europos taryba (2021) ‘EU in the global Artificial Intelligence landscape’

Prancūzija	– T. Christakis, A. Trotry (2020) 'French White Paper on Internal Security Makes Several Proposals for the Use of Facial Recognition in France' – European digital rights (2020) 'Use cases : Impermissible AI and fundamental rights breaches'. – Jobin, A., Ienca, M. and Vayena, E. (2019) 'The global landscape of AI ethics guidelines', *Nature Machine Intelligence*, 1(9), p. 389–399. – CNIL (2019) 'Facial Recognition for a Debate Living', p. 1–11. – Europos parlamentas (2020) 'Artificial Intelligence and Law Enforcement Impact on Fundamental Rights' – Council of Europe (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, p. 1–77.
Vokietija	– Gerstner, D. (2018) 'Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany', *European Journal for Security Research*, 3(2), p. 115–138. – European digital rights (2020) 'Use cases : Impermissible AI and fundamental rights breaches'. – Europos taryba (2018) 'Fostering a European approach to Artificial Intelligence', *e-conversion - Proposal for a Cluster of Excellence*, p. 29–50. – Egbert, S. (2018) 'About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany', *European Journal for Security Research*, 3(2), p. 95–114. – Egbert, S. and Krasmann, S. (2020) 'Predictive policing: not yet, but soon preemptive?', *Policing and Society*, 30(8), p. 905–919.

2 priedas „DI strategijų analizei naudotas kodų medis"

	Analizuoti dokumentai	Kodai
JK	National AI Strategy (2021)	***Siekiai-tikslai***
Prancūzija	• ETHICS OF ARTIFICIAL INTELLIGENCE (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/ethique-de-l-	***Nauda-pliusai*** ***Grėsmės-pavojus***

	intelligence-artificielle) • THE NATIONAL STRATEGY FOR AI (https://www.intelligence-artificielle.gouv.fr/fr/strategie-nationale/la-strategie-nationale-pour-l-ia) • ARTIFICIAL INTELLIGENCE AT THE SERVICE OF COMPANIES (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/l-intelligence-artificielle-au-service-des-entreprises) • AI TRAINING IN HIGHER EDUCATION (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/talents-et-competences/la-formation-ia-dans-l-enseignement-superieur) • EDUCATE ON ARTIFICIAL INTELLIGENCE (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/talents-et-competences/eduquer-l-intelligence-artificielle) • PUBLIC TRANSFORMATION AND DATA POLICY (https://www.intelligence-artificielle.gouv.fr/fr/thematiques/transformation-publique/transformation-publique-et-politique-de-la-donnee)	***Nauji projektai-iniciatyvos*** ***Esančios iniciatyvos*** ***Principai*** ***Išreikšti sunkumai-iššūkiai*** ***Į žmogų orientuotas DI***
Estija	Report of Estonia's AI Taskforce (2019)	***Kita***
Belgija	AI 4 Belgium (2021)	
Vokietija	Artificial Intelligence Strategy of the German Federal Government (2020)	

3 priedas „Tiriamų šalių naudojamos DI technologijos teisėsaugoje“

	Estijoje esamos sistemos	**Paskirtis**	**Šaltinis**
1	“Hugo-AI”	gali padėti išspręsti paprastus ar net sudėtingus teisės klausimus, padėti parengti sutartį. Kilus sudėtingoms užklausoms, HUGO suderina kliento poreikius su kvalifikuotu teisės ekspertu savo jurisdikcijoje. Taip efektyvinant procesą teisininkai gali susikoncentruoti ties savo darbo esme.	• Can AI Be a Fair Judge in Court? Estonia Thinks So https://www.wired.com/story/can-ai-be-fair-judge-court-est onia-thinks-so/ • Hugo linkedin: https://www.linkedin.com/company/hugolegalai/?original

			Subdomain=ee
2	TEXTA Toolkit	Teikia teksto analizės paslaugas: duomenų paiešką, kodavimo, išskyrimą ir kategorizavimą. Estijoje viena iš naudojimo paskirčių - neapykantos kurstančios kalbos aptikimas internete.	• Estonia: a curious and cautious approach to • Artificial intelligence and national security • TEXTA https://www.texta.ee/
3	“grėsmės vertinimo pagalbininkas ”	leis tarnybai geriau reaguoti į ekstremalias situacijas įvertinant gauto atvejo grėsmės lygį, kad būtų optimizuotas skubios pagalbos centro darbas	• Estonia: a curious and cautious approach to artificial intelligence and national security
4	“AeroVironment" "Puma 3 AE" "AeroVironment" "RQ-11 Raven" “Northrop Grumman's RQ-4 Global Hawk UAV”	Estijos organizacija "Milrem Robotics", kuri kuria bepilotes sistemas, kurios gali būti naudojamos karinėje ir civilinėje erdvėje. Tai bepiločiai orlaiviai kurie naudoja autonominius pajėgumus. Kai kurie yra naudojami NATO Aljanso antžeminės žvalgybos veikiančios Estijoje.	• Estonia: a curious and cautious approach to artificial intelligence and national security
5	"Mistral 2"	Tai oro gynyboje naudojamos trumpojo nuotolio "žemė-oras" raketos, kurios veikia autonomiškai, naudodamos funkciją "iššauti ir pamiršti" (ang. fire and forget).	• Estonia: a curious and cautious approach to artificial intelligence and national security
6	THeMIS UGV	Tai bepilotė antžeminė transporto priemonė, kuri gali būti apginkluota įvairia ginkluote, pvz.: prieštankinėmis raketomis, kulkosvaidžiais ir nuotolinio valdymo ginklų stotimis, skirtomis kovai su lengvaisiais šarvuočiais.	• Estonia: a curious and cautious approach to artificial intelligence and national security
7	Transkripcijos projektas	Naudojamas teisme, remiasi MM.	• Estonia does not develop AI Judge • https://www.just.ee/en/news/estonia-does-not-develop-ai-judge
	Vokietijoje esamos sistemos	**Paskirtis**	**Šaltinis**

1	‘PRECOBS’	Naudojama vagystėms įsilaužus į gyvenamąjį būstą prognozuoti. Remiasi nusikaltimų duomenimis, gautais iš policijos bylų apdorojimo sistemų.	• Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany • Predictive Policing in the Belgian Police Service • About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany • Predictive policing: not yet, but soon preemptive?
2	‘PreMAP’	Kaip ir PRECOBS naudojama vagystėms prognozuoti	• About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany
3	DyRiAS	Rizikos nusikalsti vertinimas pagrįstas statistine anketų analize, pateikia „grėsmės riziką“, bei asmens elgesio apžvalgą laikui bėgant ir kartu sukuria bylos dokumentaciją.	• Atlas of Automation – Automated decision-making and participation in Germany https://atlas.algorithmwatch.org/en/
4	SKALA’	naudojamos skirtingos kriminologinės teorijos vagystėms su įsilaužimu į gyvenamąsias patalpas prognozuoti, taip pat pasitelkiant nusikalstamumo duomenis ir infrastruktūrinę bei socialinę ir ekonominę informaciją.	• Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany • About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany
5	‘KLB-operativ’	"KLB-operativ" buvo sujungta su "investigator app" ("Ermittlerapp") kūrimu, kuri padeda atlikti tyrimus, išplėstinai dalijantis duomenimis. Susijusi su įsilaužimų bei vagysčių tyrimais.	• About Discursive Storylines and Techno-Fixes: The Political Framing of the Implementation of Predictive Policing in Germany • Predictive policing: not yet, but soon preemptive?
6	"hessenDATA"	Naudojama galimiems teroristams aptikti	• Predictive policing: not yet, but soon preemptive?

7	RADAR-iTE	potencialiai destruktyvių nusikaltėlių analizė, skirta ūmiai islamistinio terorizmo rizikai vertinti, t.y. "pavojingų asmenų" išpuolių rizikai nustatyti. Ši sistema įvardija tam tikro tipo asmenis kaip galimą grėsmę visuomenei, remiantis rodikliais, kurie nebūtinai susiję su nusikaltimais.	• Predictive policing: not yet, but soon preemptive?
8	'HunchLab'	Nuolat mokosi iš policijos pareigūnų pateikiamų grįžtamojo ryšio duomenų. Reguliuoja kasdienę policijos veiklą, duodama nurodymus, kaip patruliuoti. Naudoja prognozavimo metodus, pvz.: rizikos vietovės modeliavimas.	• Predictive policing: not yet, but soon preemptive? • Predictive Policing in the Context of Residential Burglary: An Empirical Illustration on the Basis of a Pilot Project in Baden-Württemberg, Germany
9	Dronai	Vokietijos oro pajėgos ir karinis jūrų laivynas taip pat naudoja įvairių tipų dronus.	• Atlas of Automation – Automated decision-making and participation in Germany https://atlas.algorithmwatch.org/en/
10	Išmanioji vaizdo stebėjimo sistema	Technologija pagrįsta ne veido atpažinimu, o automatiniu vaizdo apdorojimu. Įrengiamos kameros bus naudojamos stebėti ir skenuoti žmonių elgesį ieškant tam tikrų modelių, kurie rodo nusikalstamas veikas taip padarant kovą su gatvės nusikalstamumu veiksmingesnę ir suteikti daugiau saugumo žmonėms mieste.	• Automating society 2019 – Germany https://algorithmwatch.org/en/automating-society-2019/germany
	Prancūzijoje esamos sistemos	**Paskirtis**	**Šaltinis**
1	TAJ ("Traitement des antécédents judiciaires")	Tai duomenų bazė, naudojama atliekant teisminius ir administracinius tyrimus, joje kaupiami bylos nagrinėjimo metu surinkti duomenys, nuotraukos su techninėmis charakteristikomis, kurias gali naudoti veido atpažinimo sistemos.	• French White Paper on Internal Security Makes Several Proposals for the Use of Facial Recognition in France

2	Neįprasto elgesio fiksavimas	Ši sistema įspės policiją apie, bet kokį neįprastą elgesį, užfiksuotą vaizdo stebėjimo kameromis. Sistema kuriama siekiant nustatyti ir analizuoti elgesį, kuris gali būti laikomas neįprastu viešojoje erdvėje.	• Use cases : Impermissible AI and fundamental rights breaches
3	PARAFE	PARAFE sienos kirtimo procedūroje, asmens nuotrauka kontrolės punkte esančiame įrenginyje palyginama su asmens tapatybės dokumente (pase arba saugiame leidime gyventi) esančia nuotrauka. Naudojama veido atpažinimo funkcija kai reikia ypač aukšto lygio asmenų autentiškumo nustatymo.	• Facial recognition for a debate living up to the challenges
4	Dronai	Sprendimas susijęs su priemonėmis, leidžiančiomis fiksuoti vaizdus dronais, siekiant padėti laikytis izoliavimo ir socialinio atskyrimo priemonių. Atitinkamuose dronuose įrengta kamera ir garsiakalbis, kuriais galima perduoti pranešimus visuomenei	• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment
5	Doctrine.fr	Tai paieškos sistema. Sutvarko teisinę informaciją, kad ji būtų lengvai prieinama ir naudinga teisininkams.	• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment • https://www.appengine.ai/company/doctrine
6	Prédictice	Analizės sistema (išskyrus baudžiamąsias bylas), leidžia rūšiuoti rezultatus pagal reikšmę	• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment • https://predictice.com/fr
7	Case Law Analytics	Analizės sistema (išskyrus baudžiamąsias bylas), kuri remiasi DI ir išsamia teisine patirtimi, kad būtų galima greitai išanalizuoti riziką, susijusią su teisminio ginčo byla ar sutartimi.	• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment • https://www.caselawanalytics.com/
8	JurisData Analytics	Paieškos bei analizės sistema (išskyrus baudžiamąsias bylas), jame pabrėžiamas	• Lexis 360 - What is the difference between

	(LexisNexis)	esminis analizuojamo sprendimo teiginys, apibendrinami esminiai faktai ir glaustai pateikiamas teisėjų priimtas teisinis sprendimas.	JurisData analysis and JurisData Analytics?
			• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment
9	Artemis.IA projektas	Skaitmeninės gynybos agentūros numato sukurti keičiamo mastelio ir saugų masinio duomenų apdorojimo ir DI sprendimą.	• French DGA selects Athea for phase three of Artemis.IA project
		Suteikti Prancūzijai suverenią ir saugią didžiųjų duomenų ir dirbtinio intelekto apdorojimo platformą, galinčią išnaudoti ir analizuoti didžiulius kiekius duomenų, gaunamų iš karinės įrangos ir kitų jutiklių.	• France approves final phase of Artemis big-data processing platform
10	Automobilių vagysčių prognozė	Nacionalinės policijos ir žandarmerijos (ang. Gendarmerie) duomenų mokslininkai, naudodami dirbtinio intelekto programą, prognozuoja automobilių vagystes.	• Preventing Corruption of Civil Servants in France, Romania and the Netherlands. A comparative study of law and policy
11	ROSS	Tai sutarčių ir nuostatų peržiūra, specializuota audito srityje, siekiant aptikti abejotinas sąlygas. Taip pat padeda rasti kitas bylas su panašiomis formuluotėmis. Gali automatiškai apibendrinti byla pagal užklausos kontekstą.	• France - International Bar Association
			• Ross intelligence https://www.rossintelligence.com/features
12	RegMind	Naudoja DI, kad užtikrintų automatinę reguliavimo stebėseną ir tolesnius veiksmus bankininkystės ir finansų teisėje.	• France - International Bar Association
13	Karinės gynybos sistemos	DI pagrįstos priemonės ir ginklai, padedantys vykdyti misijas vietoje - bepiločiai orlaiviai, kurie realiuoju laiku prisitaikys prie situacijos vietoje, naikintuvai su virtualiais balso asistentais ir koviniai tankai, kuriuos gali lydėti pusiau autonominiai robotai, gebantys veikti sudėtingoje aplinkoje	• France: Artificial Intelligence Comparative Guide
14	Automatizuotas KET pažeidimų tvarkymas	Visoje Prancūzijoje dabar yra apie 4 500 radarų, kurie fiksuoja KET pažeidimus.	• Automating society 2019 – France • https://algorithmwatch.org/en/automating-society-2019/france

15	Masinis stebėjimas (ang. Mass surveillance)	Nurodo poreikį jog interneto paslaugų teikėjai įdiegtų algoritmines sistemas terorizmo grėsmėms aptikti, naudojant tik "ryšio duomenis"	• Automating society 2019 – France • https://algorithmwatch.org/en/automating-society-2019/france
16	Terorizmo grėsmių aptikimas	Įdiegta pirmoji "juodoji dėžė" (ang. Black box). Tai buvo interneto paslaugų teikėjų lygmeniu įdiegtas algoritmas, kurį žvalgybos tarnybos naudojo interneto srauto analizei, kad aptiktų terorizmo grėsmes.	• Automating society 2019 – France • https://algorithmwatch.org/en/automating-society-2019/france
	Jungtinėje karalystėje esamos sistemos	**Paskirtis**	**Šaltinis**
1	"Uber" KET pažeidimų aptikimas	Nedidelė bandomoji programa, kuri leido tikrinti ar "Uber" neviršija greičio, ar agresyviai laužė automobilį ir ar važiuodami rašė trumpąsias žinutes.	• Security News This Week: Hero Chatbot Lawyer Overturns 160,000 Parking Tickets
2	HART	Pagal dabartinį HART modelį nusikaltėliai skirstomi į tris skirtingas prognozuojamos rizikos grupes (rizikos nusikalsti), iš kurių tik viena atitinka Checkpoint gydymo reikalavimus.	• Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality • European ethical charter on the use of Artificial Intelligence in judicial systems and their environment • Use cases : Impermissible AI and fundamental rights breaches
3	"Checkpoint"	Programa siekiama šalinti pagrindines nusikalstamumo priežastis ir su tuo susijusias sveikatos ir bendruomenės problemas, siūlant alternatyvą baudžiamajam persekiojimui labai specifinei nusikaltėlių grupei. Programoje nustatomos priežastys, dėl kurių suaugęs asmuo padarė nusikaltimą, taip pat geriausios intervencijos ir paslaugos, padedančios asmeniui nutraukti nusikalstamą veiką.	• Algorithmic risk assessment policing models: lessons from the Durham HART model and 'Experimental' proportionality

4	Dronai	Nors jie daugiausia naudojami nuotoliniu bei rankiniu būdu ir ne visiškai išnaudoja DI galimybes, tačiau naudojami savadarbiams sprogstamiems užtaisams konfliktų zonose bei atakose, pvz.: siekiant sutrikdyti oro uostų veiklą Gatviko oro uoste JK 2018 m. gruodžio mėn.	• Towards responsible AI innovation
5	JK ODR platforma	Skirta ieškiniams dėl nedidelių sumų nagrinėti.	• Artificial intelligence and the judicial ruling
6	Gaujų smurto matrica (ang. Gang Violence Matrix)	Tai žvalgybos priemonė, kurią naudoja, kad nustatytų ir įvertintų gaujų narius Londone, dalyvaujančius gaujų smurte. Taip pat siekiama nustatyti asmenis, kuriems gresia viktimizacija.	• Predictive Policing in the Belgian Police Service • Gangs violence matrix • https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/gangs-violence-matrix/
7	Luminance	Analizės sistema galinti atlikti nuo bet kurios gautos sutarties pirmojo peržiūrėjimo iki automatinio žymėjimo, neatitikties sričių ištaisymo bei išryškinimo.	• European ethical charter on the use of Artificial Intelligence in judicial systems and their environment • https://www.luminance.com/
8	Nusikaltėlių grupės recidyvo skalė (ang. Offender Group Reconviction Score, OGRS)	Tai pakartotinio nusikalstamumo prognozė, pagrįsta statine rizika, pavyzdžiui, amžiumi, lytimi ir kriminaline istorija, pagal kurią apskaičiuojamos individualios prognozės. Šią priemonę taiko probacijos ir kalėjimų tarnybos visoje Europoje ir pagal algoritmą apskaičiuoja pakartotinio nusikalstamumo tikimybę	• Use cases : Impermissible AI and fundamental rights breaches
9	Nacionalinis duomenų analizės sprendimas (NDAS)	Tai rizikos vertinimo įrankis naudoja statistinę analizę ir mašininį mokymąsi policijos sprendimams pagrįsti, asmenų, kurie ateityje gali padaryti nusikaltimus, sąrašui sudaryti ir, jei reikia, ankstyvajai intervencijai palengvinti	
10	Kilmės programinė įranga (ang. Origins Software)	skirta nusikaltėlių ir nusikaltimų aukų profiliams sudaryti.	
11	Slaptas veido	Slapta, neteisėta viešojo ir privačiojo	• Use cases : Impermissible AI

	atpažinimas	sektorių partnerystė King's Cross mieste, kurią nuslėpė policija 2018 m.	and fundamental rights breaches
12	"Nacionalinė sukčiavimo iniciatyva"	JK vyriausybė pradėjo nacionalinę automatinę (iš jiems prieinamų asmens duomenų šaltinių) duomenų palyginimo iniciatyvą, kuria siekiama surasti sukčiaujančius pašalpų mokėtojus.	• Preventing corruption of civil servants in France, Romania and the Netherlands
	Belgijoje esamos sistemos	**Paskirtis**	**Šaltinis**
1	Veido atpažinimo kameros	Belgijoje DPA (ang. Data Protection Authority) ir teismas sustabdė veido atpažinimo kamerų diegimą Zaventemo oro uoste, kuris neturėjo jokio teisinio pagrindo	• Artificial Intelligence and Law Enforcement Impact on Fundamental Rights
2	Prognostinės policijos veiklos projektas	Esmė, kad policijos zona, remdamasi prognozėmis, žino, kuri zonos vieta yra vagysčių ir kitų nusikaltimų rizikos zona.	• Use cases : Impermissible AI and fundamental rights breaches
3	“iPolice”	Šia Sistema bus vykdoma prognozuojamoji policijos veikla. Jai naudojami duomenų bankai ir algoritmai, padedantys nustatyti laiką ir vietas, kada ir kur yra padidėjusi nusikalstamos veiklos tikimybė.	• Use cases : Impermissible AI and fundamental rights breaches
4	"Luminance"	DI pagrįsta dokumentų analizės platforma, kurioje naudojamas galingas MM, algoritmai ir modelių atpažinimas, kad būtų galima greitai analizuoti teisinius dokumentus. Išryškindama anomalijas ir nustatydama riziką, platforma leidžia greitai peržiūrėti didelius dokumentų kiekius. Šiuo požiūriu technologija bus ypač naudinga atliekant teisinį išsamų patikrinimą.	• EY Law Belgium embraces Artificial Intelligence (AI) for legal document review

5	“2KnowHow2”	Sistema padeda teisinių paslaugų teikėjams optimizuoti savo žinias, kad vidaus ir išorės klientams galėtų teikti inovatyvesnes paslaugas ir produktus.	• Innovations in the legal services supported by the use of visual law: the reality in Finland and Belgium
6	“GPT-3”	DI algoritmas galintis generuoti tekstą, supaprastinti, apibendrinti ir suasmeninti. Jis gali išversti teisinę kalbą į paprastą kalbą ir atvirkščiai.	• Innovations in the legal services supported by the use of visual law: the reality in Finland and Belgium
7	Įsilaužimų bei vagysčių prognostika	Remdamasi policijos gaunamais duomenimis, sistema gali numatyti, kuriuose rajonuose yra didesnė tikimybė, kad bus įvykdyta vagystė su įsilaužimu. Remdamiesi šia prognoze, jie siunčia intervencijos grupę.	• Automating society 2019 – Belgium
8	Automatinis numerių atpažinimas (ANPR)	Norima išplėsti prognostinę vagysčių bei įsilaužimų aptikimo sistemą į ją įtraukiant kameras, kurios automatiškai atpažįsta numerius	• Automating society 2019 – Belgium
9	Dronai/ bepiločiai orlaiviai	Belgijos gynybos srityje sparčiai augantis susidomėjimas. Į tai įeina ir mini bei taktiniai bepiločiai orlaiviai naudojami karinėje ir šalies gynybos srityje.	• Belgian army to buy RQ-20 Puma and RQ-21 Integrator drones • Hadron https://mecatron.rma.ac.be/index.php/projects/hadron/