



Veido atpažinimo technologijų naudojimas teisėsaugos srityje: teisiniai iššūkiai ir galimi sprendimai

Mokslinio projekto tyrimais grįstos
rekomendacijos

Dr. Rita Matulionytė

Dr. Agnė Limantė

Dr. Eglė Kavoliūnaitė-Ragauskienė



LIETUVOS SOCIALINIŲ
MOKSLŲ CENTRO
TEISĖS INSTITUTAS

2023

Veido atpažinimo technologijų naudojimas teisėsaugos srityje: teisiniai iššūkiai ir galimi sprendimai

Mokslinio projekto tyrimais grįstos
rekomendacijos

Rita Matulionytė

Agnė Limantė

Eglė Kavoliūnaitė-Ragauskienė



Lietuvos socialinių mokslyų centro Teisės institutas,
Vilnius, 2023

Autorės (Lietuvos socialinių mokslų centro Teisės institutas):

dr. Rita Matulionytė (projekto vadovė),

dr. Agnė Limantė,

dr. Eglė Kavoliūnaitė - Ragauskienė.

Kalbos redaktorė dr. Dalia Gedzevičienė

Leidinio dizaino kūrėja Goda Dainauskaitė

Leidinio maketuotojas Rimantas Junevičius



Lietuvos
mokslo
taryba

Projektą „Veido atpažinimo technologijos valstybės institucijų veikloje: teisiniai iššūkiai ir galimi sprendimai“ (VeidAI) ir jo pagrindu parengtų rekomendacijų leidybą pagal Lietuvos mokslo tarybos veiklos kryptį „Mokslininkų grupių projektai“ finansavo Lietuvos mokslo taryba (LMT), sutarties Nr. S-MIP-21-38.

ISBN 978-609-8324-05-1

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



LIETUVOS SOCIALINIŲ
MOKSLŲ CENTRO
TEISĖS INSTITUTAS

© Rita Matulionytė, Agnė Limantė,

Eglė Kavoliūnaitė-Ragauskienė, 2023

© Lietuvos socialinių mokslų centro Teisės institutas, 2023

TURINYS

ĮVADAS.....	4
DOKUMENTO RENGĖJOS.....	5
1. PAGRINDINIAI VAT NAUDOJIMO VIEŠAJAME SEKTORIUJE BŪDAI	7
1.1. VAT naudojimas tapatybės nustatymo ir (arba) tikrinimo tikslais.....	7
1.2. VAT naudojimas nežinomam asmeniui identifikuoti.....	8
1.3. VAT, skirtos naudoti realiuoju laiku viešosiose erdvėse	8
1.4. Pasitelkus VAT atliekamas kategorizavimas	9
1.5. VAT naudojimas emocijoms atpažinti	10
2. VAT NAUDOJIMO TEISÉSAUGOS INSTITUCIJOSE IŠŠÜKIAI.....	11
2.1. Duomenų apsauga ir asmens teisė į privatumą.....	11
2.2. Šališkumas ir (arba) diskriminacija.....	13
2.3. Saviraiškos ir asociacijos laisvės.....	16
2.4. Skaidrumas	17
3. NAUJAUSIOS POLITINĖS IR TEISINĖS INICIATYVOS VAT SRITYJE	20
3.1. Pasaulio ekonomikos forumo Politikos programa dėl atsakingo veido atpažinimo technologijų naudojimo.....	20
3.2. ES dirbtinio intelekto aktas.....	21
3.3. Europos duomenų apsaugos valdybos gairės dėl VAT teisėsaugos srityje	22
3.4. Europos Tarybos gairės dėl VAT naudojimo	23
3.5. Iniciatyvos Jungtinėje Karalystėje	23
3.6. Iniciatyvos Naujojoje Zelandijoje ir Australijoje	24
4. REKOMENDACIJOS.....	26
4.1. Aiškus ir konkretus teisinis pagrindas	26
4.2. Pagarba žmogaus teisėms.....	27
4.3. Kokybės užtikrinimas.....	28
4.4. Nuolatinė priežiūra ir atskaitomybė	28
4.5. Skaidrumas ir visuomenės informuotumo didinimas.....	29
4.6. Profesinis mokymas.....	30
BIBLIOGRAFIJA.....	31

IVADAS

Vis daugiau teisėsaugos institucijų visame pasaulyje naudoja veido atpažinimo technologijas (toliau – VAT). Šios modernios priemonės gali prisišteti prie visuomenės saugumo, nusikaltimų ir teroristinių išpuolių prevencijos arba palengvinti dingusių žmonių ar įtariamujų paiešką. Visgi, nepaisant didelio potencialo, VAT gali kelti ir nemažai teisinių rizikų. Netinkamas VAT taikymas gali lemti privatumo ir duomenų apsaugos įstatymų pažeidimus ar padidinti šališkumo ir diskriminacijos tikimybę. Šios technologijos taip pat gali būti naudojamos viešiems protestams ir saviraiškos laisvei slopinti. VAT gali trūkti skaidrumo, todėl gali būti priimami nepaaiškinami ir klaudingi sprendimai, sukeliama žala asmenims.

Šių rekomendacijų tikslas – apibendrinti ir paaiškinti pagrindines galimas teisines rizikas, kylančias naudojant VAT teisėsaugos srityje, ir pasiūlyti galimus sprendimus, kaip šias rizikas valdyti tobulinant VAT naudojimo politiką ir teisinį reguliavimą.

Šios rekomendacijos – tai projekto „Veido atpažinimo technologijos valstybės institucijų veikloje: teisiniai iššūkiai ir galimi sprendimai“ (VeidAI) rezultatas. Projektui finansavimą skyrė Lietuvos mokslo taryba (LMTLT) (sutarties Nr. S-MIP-21-38). Projekto rezultatai grindžiami 32 interviu su nacionaliniais ir tarptautiniais veido atpažinimo technologijų ekspertais, dirbančiais teisėsaugos, politikos, akademiniame ir NVO sektoriuose, bei lyginamaja teisine analize, kuria siekta nustatyti, kaip VAT taikomos skirtingoje jurisdikcijoje (Europoje, JAV, Azijoje, Australijoje, Naujojoje Zelandijoje), kokios rizikos buvo identifikuotos bei kaip jos buvo valdomos.

Šį dokumentą sudaro keturios dalys. Pirmojoje dalyje pristatomos VAT ir aptariaimi įvairūs šių technologijų naudojimo būdai valdžios, ypač teisėsaugos, institucijose. Antrojoje dalyje įvardijamos su šiomis technologijomis susijusios galimybės ir iššūkiai, daugiausia dėmesio skiriant teisei į privatumą, galimam VAT ir jų naudojimo šališkumui ir diskriminavimui, įtakai politinėms laisvėms bei VAT skaidrumui. Trečiojoje dalyje apžvelgiamos kai kurios naujausios politinės ir teisinės iniciatyvos, skirtos su VAT susijusiomis etinėms ir teisinėms rizikoms įvairose jurisdikcijoje mažinti. Galiausiai paskutinėje dalyje pateikiamos rekomendacijos, kaip derėtų spręsti su VAT susijusias rizikas ir kaip sudaryti sąlygas etiškam ir teisiškai tinkamam šių technologijų pasitelkimui visuomenės labui.

DOKUMENTO RENGĖJOS

Dr. Rita Matulionytė yra Lietuvos socialinių mokslų centro Teisės instituto vyriausioji mokslo darbuotoja ir Makvairo universiteto (Australija) Teisės mokyklos vyresnioji dėstytoja. Ji yra tarptautinė intelektinės nuosavybės ir technologijų teisės ekspertė, o jos naujausi tyrimai analizuoją teisinius ir valdymo klausimus, susijusius su dirbtinio intelekto technologijomis. Dr. R. Matulionytė yra paskelbusi daugiau nei 50 mokslinių straipsnių pirmaujančiuose žurnaluose ir tarptautinėse leidyklose, ji buvo kviečiama pristatyti savo tyrimus konferencijose Europoje, Azijoje, JAV ir Australijoje. Ji yra viena iš Europos patentų biurui, Pietų Korėjos ir Australijos vyriausybėms rengtų ataskaitų bendraautorė. R. Matulionytė vadovauja Australazijos kompiuterių ir teisės draugijos (AUSCL) darbo grupei „Naujosios technologijos“, Makvairo universiteto Taikomojo dirbtinio intelekto centro Dirbtinio intelekto paaškinamumo tyrimų grupei ir yra aktyvi Australijos dirbtinio intelekto aljanso sveikatos priežiūros srityje narė.

Dr. Agnė Limantė yra Lietuvos socialinių mokslų centro Teisės instituto vyriausioji mokslo darbuotoja. Ji įgijo ES teisės magistro laipsnį Karališkajame Londono koledže (apdovanota prizu už geriausią ES teisės magistro darbą) ir daktaro laipsnį Vilniaus universitete. Dr. A. Limantė yra žmogaus teisių ekspertė ir yra paskelbusi daugiau kaip 40 straipsnių, įskaitant straipsnius nacionaliniuose ir tarptautiniuose žurnaluose bei knygų skyrius prestižinėse leidyklose. A. Limantė yra dėčiusi Vilniaus universitete, Europos humanitariniame universitete, Kauno technologijos universitate ir Khazaro universitete (Azerbaidžane). Dr. A. Limantė taip pat turi daug patirties dirbant tarptautinėse komandose ir atliekant lyginamuosius tyrimus. Ji aktyviai dalyvauja ES moksliniuose bei ekspertiniuose projektuose, dažnai vadovaudama naciona-linei komandai, bei nacionaliniuose moksliniuose projektuose.

Dr. Eglė Kavoliūnaitė-Ragauskienė yra Lietuvos socialinių mokslų centro Teisės instituto mokslo darbuotoja. Ji yra paskelbusi daugiau nei 30 mokslinių straipsnių, dirbusi ties įvairiaisiais teisinio reguliavimo, viešojo administravimo ir politikos formavimo klausimais, įskaitant Viešojo atskaitingumo mechanizmų (PAM) iniciatyvą (Pasaulio bankas, 2010 m.); Pasaulinę sąžiningumo ataskaitą 2008 (*Global Integrity*, 2008 m.); *EU Profiler* (Romano Šumano pažangiuju studijų centras, Europos univer-

sitetinis institutas, 2009 m.); *EUandI* (Europos universitetinis institutas, 2014 m.); ES valstybių narių konsultacijas su pilietine visuomene Europos politikos klausimais (Europos universitetinis institutas, 2010 m.). Dr. E. Kavoliūnaitė-Ragauskienė skaitė paskaitas Mykolo Romerio bei Vytauto Didžiojo universitetuose, vedė mokymus teisėjams, advokatams bei teisėsaugos pareigūnams.

1. PAGRINDINIAI VAT NAUDOJIMO VIEŠAJAME SEKTORIUJE BŪDAI

VAT – tai biometrinės sistemos, leidžiančios automatiškai atpažinti asmens veidą. Nuskenuodami ir atlikdami veido bruožų matavimus bei palygindami gautus duomenis su kitais turimais duomenimis, algoritmai leidžia sekundžių ar minučių greičiu gauti atsakymą, ar du pateikti atvaizdai yra to paties asmens. Taip tokio tipo dirbtinis intelektas supaprastina daugelį kasdienių veiksmų tiek privatiems, tiek viešiesiems subjektams, padėdamas šiemis įgyvendinti jų funkcijas bei atlirkti įvairias užduotis.

Dažniausiai VAT naudojamos tapatybės patvirtinimo ir (arba) patikrinimo, identifikavimo ir kategorizavimo tikslais. Toliau trumpai aptariami šie VAT naudojimo būdai.

1.1. VAT naudojimas tapatybės nustatymo ir (arba) tikrinimo tikslais

Tapatybės nustatymo ar tikrinimo (autentifikavimo) atveju dirbtinio intelekto algoritmai palygina iš anksto į sistemą įrašytus biometrinius duomenis su vienu konkrečiu veidu ir nustato, ar tai tas pats asmuo. Pavyzdžiui, VAT gali būti naudojama asmeniniuose įrenginiuose – tai veiksmas, kurį daugelis mūsų atliekame kelis kartus per dieną, norédami atrakinti savo išmanujį telefoną arba vieną iš jo programėlių.

VAT taip pat gali būti naudojamos sienos perėjimo punktuose tapatybei nustatyti bei siekiant patikrinti asmens tapatybę pagal jo kelionės dokumentus. Šiuo tikslu kontrolės poste asmuo nuskenuoja savo pasą, o kamera užfiksuoja tiesioginę nuotrauką. Tada VAT palygina du veido atvaizdus, įvertindamos tikimybę, kad abiejuose atvaizduose yra užfiksotas tas pats asmuo. Paminėtina, kad ES reglamente, kuriuo sukuria ma atvykimo ir išvykimo sistema (AIS)¹, veido atvaizdai buvo įvardinti kaip biometri niai identifikatoriai ir numatyta, kad VAT gali būti naudojamos patikros tikslais.

¹ 2017 m. lapkričio 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2226, kuriuo sukuriama atvykimo ir išvykimo sistema (AIS), kurioje registruojami trečiųjų šalių piliečių, kertančių valstybių na rių išorės sienas, atvykimo ir išvykimo beiatsisakymo leisti jiems atvykti duomenys, nustatomos prieigos

1.2. VAT naudojimas nežinomam asmeniui identifikuoti

Teisėsaugos institucijos įvairiose šalyse dažnai naudoja VAT asmeniui (pvz., įtariamajam arba aukai) identifikuoti. Turint asmens veido atvaizdą, biometrinis profilis lyginamas su informacija specifinėje (pvz., ieškomų asmenų bazėje) ar bendrojoje duomenų bazėje (pasū, vairavimo teisių duomenų bazėse)². Kartais atvaizdai gali būti tikrinami žinant, kad šioje duomenų bazėje tikrinamo asmens veido atvaizdas yra (uždarojo rinkinio tapatybės nustatymas); tačiau kartais nežinoma, ar asmuo yra ištrauktas iš konkrečią duomenų bazę – taip yra, pavyzdžiui, kai asmenys tikrinami pagal ieškomų asmenų sąrašus (atvirojo rinkinio tapatybės nustatymas)³.

Palyginus asmens veido atvaizdą su kitais duomenų bazėje saugomais atvaizdais, veido atpažinimo technologija suranda artimiausią atitikmenį ar keli galimus variantus nurodydama tikimybę, kad du atvaizdai yra to paties asmens. Tai ypač naudinga atliekant kriminalinį tyrimą, kai gaunama įtariamojo nuotrauka ir policija siekia nustatyti nežinomo asmens tapatybę.

1.3. VAT, skirtos naudoti realiuoju laiku viešosiose erdvėse

VAT taip pat gali būti naudojamos nuotoliniam biometriniam atpažinimui realiuoju laiku, kai praeivio atvaizdas tikrinamas duomenų bazėje. Tai paprastai atliekama siekiant nustatyti asmenis, ištrauktus iš stebimų ar ieškomų asmenų sąrašą. Tokiu atveju veido atpažinimo kameros veikia skenuodamos ir matuodamos visų praeivų veidus. Duomenys įrašomi ir kiekvienam asmeniui suteikiamas unikalus atpažistomas skaitmeninis kodas. Jei gauti duomenys sutampa su stebimų ar ieškomų asmenų sąraše esančiu atvaizdu (sistema „atpažista asmenį“), veido atpažinimo sistema pateikia perspėjimą.

Šios sistemos – vadinamosios tikralaikio nuotolinio veido atpažinimo technologijos (angl. *live facial recognition technologies*) – yra labiau prieštaringos nei jau aptartos VAT naudojimo galimybės, nes jos leidžia vykdyti masinį stebėjimą viešosiose erdvė-

prie AIS teisėsaugos tikslais sąlygos ir iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir reglamentai (EB) Nr. 767/2008 ir (ES) Nr. 1077/2011. OJ L 327, 9.12.2017, p. 20–82.

² Daugelis veido atpažinimo duomenų bazių yra sukurtos iš administracinių duomenų bazių, pavyzdžiui, vairuotojų pažymėjimų nuotraukų duomenų bazių. Marcus Smith, Monique Mann ir Gregor Urbas, *Biometrics, Crime and Security* (Taylor & Francis 2018), 4 skyrius.

³ FRA, „Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (žiūrėta 2023 m. kovo 30 d.).

se. Skirtingai nuo kitų biometrinių sistemų, pavyzdžiui, pirštų atspaudų ar akies rai-nelės atpažinimo technologijų, VAT nereikalauja stebimų asmenų žinios, sutikimo ar aktyvaus dalyvavimo. Tad daug asmenų gali būti fiksuojami ir tikrinami, nors jie nėra įtraukti į stebimą ar ieškomą asmenų sąrašą ir net nežino apie tokį stebėjimą. Ar tai būtų sporto renginys, protestas, ar tiesiog miesto centras ir jo judrios gatvės – tikralaikio nuotolinio veido atpažinimo technologijos gali būti kur nors netoli ese, rinkti duomenis apie renginio dalyvius ar praeivius ir juos analizuoti.

Tikralaikio nuotolinio veido atpažinimo technologijų naudojimas gali daryti reikšmingą poveikį demokratijai, teisinės valstybės principui, individualioms laisvėms, todėl ši galimybė yra sulaukusi daug kritikos. Nors kai kuriose šalyse (pvz., Kinijoje, Rusijoje) ji plačiai naudojama, Europos Sąjungoje tikralaikio nuotolinio veido atpažinimo technologijos pasitelkiamos itin ribotai. Pagal ES dirbtinio intelekto akto projektą (2021 m.)⁴, būtų draudžiamas tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemų naudojimas viešosiose erdvėse teisėsaugos tikslais, išskyrus atvejus, kai taikomos tam tikros ribotos išimtys.

1.4. Pasitelkus VAT atliekamas kategorizavimas

VAT taip pat gali būti naudojamos asmenims profiliuoti ir skirstyti į kategorijas pagal jų asmenines savybes. Kategorizavimo metu iš esmės nustatoma, ar asmuo priklauso tam tikrai grupei pagal jo biometrines savybes, pavyzdžiui, lytį, amžių ar rasę⁵. Kategorizavimas taip pat gali būti atliekamas ir pagal mažiau akivaizdžias asmens savybes, pavyzdžiui, politines pažiūras, seksualinę orientaciją⁶, kurias, pasak VAT šalininkų, taip pat galima (iš dalies) nustatyti pagal veido atvaizdą.

Toks asmenų skirstymas pasitelkus dirbtinį intelektą gali turėti įtakos teisiniams ir politiniams sprendimams ir net nacionalinio saugumo priemonėms. Tai gali lemti ne tik konkrečių asmenų ar asmenų grupės diskriminavimą, bet ir naudojimosi laisvėmis aprūpojimus, ypač jei VAT taikymo rezultatai lemtų, kad tam tikros teisės asmeniui yra nesuteikiamos arba aprūpojamos.

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

⁵ FRA, „Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (žiūrėta 2023 m. kovo 30 d.).

⁶ Yilun Wang ir Michal Kosinski, „Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images“ (2018) 114 Journal of Personality and Social Psychology 246. Prieiga per internetą: <http://doi.apa.org/getdoi.cfm?doi=10.1037/pspa0000098> (žiūrėta 2023 m. sausio 21 d.).

1.5. VAT naudojimas emocijoms atpažinti

Moderniosios VAT taip pat gali būti naudojamos asmens nuotaikai ar emocijoms atpažinti, nustatant, pavyzdžiui, ar asmuo agresyvus, ar jis sako tiesą⁷. Nors šiuo metu veido išraiškos analizės technologija dar nėra tokia pažangi kaip automatinis veido atpažinimas, tačiau tai yra besivystanti sritis, galinti būti plačiai taikoma nusikalstamumo ir saugumo srityje⁸.

Tokios technologijos bandymą 2020 m. jau atliko Linkolnšyro policija (Jungtinė Karalystė)⁹. 2018 m. Manheime (Vokietija) vietas policija įrengė kameras, skirtas asmenų judėjimui fiksuoти. Judėjimo modeliai analizuojami ieškant įtartino elgesio¹⁰. Galimas VAT panaudojimas siekiant nustatyti, ar asmuo nemeluoją, buvo tirtas prie pasirinktų ES išorės sienų (Graikijoje, Vengrijoje ir Latvijoje). Tai buvo daroma vykdant kontroversišką *Intelligent Portable Border Control System (iBorderCtrl)* projekta, kuriami integravotos veido atpažinimo ir kitos technologijos, leidžiančios nustatyti, ar asmuo sako tiesą¹¹.

⁷ Taip pat žr.: „TechDispatch #1/2021 - Facial Emotion Recognition | European Data Protection Supervisor“ (1 February 2023). Prieiga per internetą: <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition> (žiūrėta 2023 m. vasario 6 d.).

⁸ Marcus Smith, Monique Mann ir Gregor Urbas, *Biometrics, Crime and Security* (Taylor & Francis 2018), 4 skyrius.

⁹ Nicholas Fletcher, „Lincs Police to Trial New CCTV Tech That Can Tell If You're in a Mood“ (*LincolnshireLive*, 17 August 2020). Prieiga per internetą: <https://www.lincolnshirelive.co.uk/news/local-news/new-lincolnshire-police-cctv-technology-4431274> (žiūrėta 2022 m. lapkričio 21 d.); Article 19.org, „Emotion Recognition Technology Report“ (ARTICLE 19, 2021). Prieiga per internetą: <https://www.article19.org/emotion-recognition-technology-report/> (žiūrėta 2022 m. lapkričio 22 d.).

¹⁰ Greens Efa, „Facial Recognition in European Cities - Read Our New Study“ (Greens/EFA, 22 October 2021). Prieiga per internetą: <https://www.greens-efa.eu/opinions/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/> (žiūrėta 2023 m. vasario 6 d.).

¹¹ „Home | iBorderCtrl“. Prieiga per internetą: <https://www.iborderctrl.eu/> (žiūrėta 2023 m. vasario 6 d.).

2. VAT NAUDOJIMO TEISÉSAUGOS INSTITUCIJOSE IŠŠŪKIAI

Dėl nuolatinio VAT tobulėjimo (ypač tapatybės nustatymo, identifikavimo srityse) atsiranda vis daugiau socialiai naudingų šių technologijų panaudojimo galimybių. Tinkamai naudojamos VAT gali padidinti teisėsaugos veiklos veiksmingumą ir ekonomiškumą. Šis dirbtinis intelektas gali padėti užkirsti kelią terorizmui, mažinti nusikalstamumą, greičiau nustatyti ieškomų ar dingusių asmenų buvimo vietą. Vis dėlto pripažįstama, kad VAT kelia nemažai etinių ir teisinių iššūkių. Toliau aptariame keturis pagrindinius aspektus: iššūkius, susijusius su privatumu, galimu šališkumu ir diskriminavimu, su politinėmis teisėmis susijusias rizikas ir skaidrumo poreikį.

2.1. Duomenų apsauga ir asmens teisė į privatumą

Veido atpažinimo sistemos leidžia greitai aptikti ieškomus veidus žmonių minioje, apibūdinti juos (nustatyti rasę, etninę priklausomybę, asmenines emocijas ir pan.) ir nustatyti asmens tapatybę. Kaip minėta, pastarasis veiksmas galimas atliekant 1:N tapatybės patikrinimą (t. y. patvirtinant asmens tapatybę pagal jau įrašytą biometrinį duomenų kodą, žr. 1.1 skyrių); VAT taip pat leidžia nustatyti asmenų tapatybę atliekant 1:N tapatybės nustatymą (t. y. siekiant identifikuoti nežinomą asmenį asmens biometrinius duomenis lyginant su didele biometriniių duomenų baze, žr. 1.2 skyrių).

Diegiant VAT viešose vietose, teisė į privataus gyvenimo gerbimą ir duomenų apsaugą yra itin svarbios. Nors šios dvi teisės glaudžiai susijusios, jos yra atskiros ir savarankiškos. Tiesioginio veido atpažinimo technologijų naudojimas viešose erdvėse reiškia, kad veido atvaizdai renkami, lyginami ir (arba) saugomi IT sistemoje atpažinimo tikslais. Todėl tai yra kišimasis į ES pagrindinių teisių chartijos 8 straipsnyje nustatytą teisę į asmens duomenų apsaugą ir teisę į privatų gyvenimą pagal Chartijos 7 straipsnį ir Europos žmogaus teisių konvencijos 8 straipsnį¹². Pažymėtina, kad nors privataus

¹² FRA, „Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf.

gyvenimo sąvoka plati ir negali būti išsamiai apibrėžta, ji taip pat apima asmens sąveikos su kitais asmenimis sritį, net jei ši sąveika vyksta viešoje erdvėje. Tobulėjant veido atpažinimo technologijoms, veido atvaizdų apdorojimas didelės apimties duomenų bazėse gali kelti neišspręstų klausimų, susijusių su teise į privatų gyvenimą ir asmens duomenų apsauga¹³. Atsižvelgiant į tai, kad šios dvi teisės nėra absoliučios, joms gali būti taikomi apribojimai, tačiau bet koks įsikišimas turi būti tinkamai pagristas ir negali paneigti šių teisių.

Atkreiptinas dėmesys į tai, kad yra įvairių veido atpažinimo technologijų, todėl skiriasi ir jų poveikis asmens teisei į privatumą. VAT grindžiamos skirtingomis asmenų biometriniių duomenų bazėmis (pvz., duomenų bazėmis, sukurtomis iš viešai prieinamų šaltinių, išskaitant socialinius tinklus, pvz., „Clearview“ duomenų bazę; valstybės registrų duomenimis ir t. t.). Be to, jos yra skirtinę tikslumo lygių (pvz., skirtinę galimybių pateikti tikslų rezultatą priklausomai nuo asmens etninės priklausomybės ar lyties), skirtinę tipų ir pan. Taip pat asmens teisės į privatumą ir suderinamumo su teisinės valstybės principais požiūriu svarbu atskirti vaizdo stebėjimo ir veidų atpažinimo įrangą, galinčią nustatyti asmens tapatybę realiuoju laiku (vadinamosios tikralaikio nuotolinio veido atpažinimo technologijos – žr. 1.3 skyrių), nuo technologijų, skirtų nustatyti asmens tapatybę iš filmuotos ar fotografiuotos medžiagos. Skirtinės VAT daro skirtinę poveikį teisei į privatumą.

Europoje biometriniams asmens duomenims taikomas specialus ir griežtesnis apsaugos režimas nei įprastiems asmens duomenims. Pagal teisės aktuose pateiktas apibarėžtis biometriniai duomenys – tai po specialaus techninio apdorojimo gauti asmens duomenys, susiję su fizinio asmens fizinėmis, fiziologinėmis arba elgesio savybėmis, pagal kurias galima konkrečiai nustatyti arba patvirtinti to fizinio asmens tapatybę, kaip antai veido atvaizdai arba daktiloskopiniai duomenys¹⁴. ES lygmeniu pagal Bendrajį duomenų apsaugos reglamentą¹⁵ (išskaitant Duomenų apsaugos teisėsaugos srityje direktyvą¹⁶) biometriniai duomenys yra tik tie duomenys, kurie buvo apdoroti speci-

¹³ *Ibid.*

¹⁴ 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119, 4.5.2016, p. 1–88. Šis apibarėžtis pateikiamas 4(14) straipsnyje.

¹⁵ *Ibid.*

¹⁶ 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. OL L 119, 2016 5 4, p. 89–131.

finiu techniniu būdu. Tai leidžia teigti, kad tokie asmens duomenys, kaip veido atvaizdas, balsas, eisena ir kiti požymiai, laikomi įprastais asmens duomenimis, kol jie nėra tvarkomi specialiomis priemonėmis, ir jiems netaikomas biometrinių duomenų apsaugos režimas.

Taigi, įprastai užfiksavus veido atvaizdą tokių asmens duomenų tvarkymui taikomos įprastos duomenų tvarkymo taisyklės. Be to, leidžiama fotografiuoti asmenis višejoje vietoje be jų sutikimo. Dauguma atvejų, kalbant apie viešas vietas¹⁷, žmogaus atvaizdų fiksavimas ir kaupimas iš esmės nėra reguliuojamas ar ribojamas. Tik tuo atveju, kai asmens atvaizdas tvarkomas veido atpažinimo technologijų programa, jam turės būti taikomas biometrinių duomenų tvarkymo taisyklės. Tačiau atsižvelgiant į tai, kad veido atpažinimo technologijos būna ne tik atpažįstančios veidą realiuoju laiku, bet ir galinčios apdoroti įprastomis vaizdo fiksavimo priemonėmis fiksuočius atvaizdus, kyla didelis pavojus, kad masiškai renkami žmogaus atvaizdai duomenų bazėse dėl klaidos ar neteisėtų veiksmų gali būti apdoroti veido atpažinimo technologijomis, ir taip gavus biometrinius asmens duomenis asmenų tapatybės gali būti atskleistos. Todėl siekiant apsaugoti asmens privatumą ypač daug dėmesio turi būti skirta siekiant užtikrinti biometrinių duomenų apsaugą, atsižvelgiant į duomenų tvarkymui naudojamą technologiją.

2.2. Šališkumas ir (arba) diskriminacija

Kitas iššūkis, susijęs su VAT, yra galimas VAT šališkumas ir diskriminacinis poveikis. Teisėsaugos institucijų neobjektyvumas ir šališka (rasistiška) policijos pareigūnų veikla įvairiose valstybėse buvo ne kartą nagrinėjami mokslinėje literatūroje, politikos dokumentuose ir kitur¹⁸. Nors kartais linkstama manyti, kad naudojant technolo-

¹⁷ Žr. Lietuvos Respublikos visuomenės informavimo įstatymas. Valstybės žinios, 1996-07-26, Nr. 71-1706. 13 straipsnis.

¹⁸ Paminėsime tik kelis naujausius mokslinius straipsnius: Lois James, „The Stability of Implicit Racial Bias in Police Officers“ (2018) 21 Police Quarterly 30. Prieiga per internetą: <https://doi.org/10.1177/1098611117732974> (žiūrėta 2022 m. lapkričio 16 d.); Dean Knox, Will Lowe ir Jonathan Mummolo, „Administrative Records Mask Racially Biased Policing“ (2020) 114 American Political Science Review 619. Prieiga per internetą: https://www.cambridge.org/core/product/identifier/S0003055420000039/-type/journal_article (žiūrėta 2022 m. lapkričio 16 d.); Kristina Murphy ir kiti, „Police Bias, Social Identity, and Minority Groups: A Social Psychological Understanding of Cooperation with Police“ (2018) 35 Justice Quarterly 1105. Prieiga per internetą: <https://doi.org/10.1080/07418825.2017.1357742> (žiūrėta 2022 m. lapkričio 16 d.); P Jeffrey Brantingham, Matthew Valasik ir George O Mohler, „Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial“ (2018) 5 Statistics and Public Policy 1. Prieiga per internetą: <https://doi.org/10.1080/2330443X.2018.1438940> (žiūrėta 2022 m. lapkričio 16 d.).

logijas ir algoritmus šališkumas sumažės ar net išnyks (nes šališkumą mes siejame su žmogaus išankstiniiais nusistatymais), tokia prielaida yra klaudinanti. Daugybė studijų parodė, kad VAT gali būti šališkos, t. y. jos dažnai tiksliai identifikuojant vienas grupes asmenį (pvz., baltaodžius, vyrus) ir mažiau tiksliai identifikuojant kitas grupes asmenį (pvz., tamsejnės odos asmenis, moteris). Kaip savo baltojoje knygoje „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ pažymėjo Europos Komisija, nesant socialinės kontrolės mechanizmų, kurie reguliuoja žmogaus elgesį, dirbtinio intelekto neobjektyvumas gali turėti kur kas didesnį poveikį, neigiamai paveikti ir diskriminuoti daug žmonių¹⁹. Algoritminis šališkumas kelia ypatingą susirūpinimą, kai dėl jo atliekamos kratos ir suėmimai, pagrįsti klaudinga identifikacija, arba kai remdamosi dirbtinio intelekto pateikiamomis išvadomis viešosios ir privačios organizacijos tiesiogiai ar netiesiogiai diskriminuoja mažumų grupes ir jų narius. Pavyzdžiui, vienas pirmųjų viešai diskutuotų neteisėtų suėmimų, įvykusį dėl neteisingo VAT identifikavimo, buvo juodaodžio R. Williams'o suėmimas JAV 2020 m. – šis įvykis tapo pavyzdžiu, kaip VAT klaida gali lemти visiškai nesusijusio asmens sulaikymą²⁰. Jei tam tikroms etninėms grupėms priklausantys asmenys neproporcingai dažnai klaudingai sustabdomi, tokios klaudos gali turėti neigiamą poveikį grupių sanglau-dai bei turėti reikšmingą įtaką jų pasitikėjimui policija ar pareigūnais.

Diskriminacijos draudimo principas VAT kontekste iš esmės reiškia, kad visiems asmenims, kuriems taikomos VAT, turi būti taikomos vienodos sąlygos. Skirtingas požiūris (vertinimas) neturėtų kilti nei iš paties algoritmo, nei diegiant ar naudojant VAT priemones. Šiuo atžvilgiu išskirtinos dvi priežastys, galinčios kelti VAT šališkumą: duomenų perspektyva (pačių VAT tikslumas arba techninis veikimas) ir socialinė perspektyva (tai, kaip ši technologija pasitelkiama viešųjų institucijų veikloje)²¹.

Kalbant apie *duomenų perspektyvą*, neobjektyvumas ir diskriminavimas dirbtinio intelekto technologijose gali atsirasti kuriant, testuojant ir diegiant algoritmus. Pavyzdžiui, šališkumas gali atsirasti dėl mokymo duomenų rinkinio, sistemos dizaino ar dėl techninio šališkumo, atsirandančio dėl supaprastinimo, kurio reikia norint tikro-

¹⁹ Europos Komisija. „Baltoji knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“. COM (2020) 65 final, p. 13. Prieiga per internetą: <https://op.europa.eu/lt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa-75ed71a1> (žiūrėta 2023 m. kovo 29 d.).

²⁰ Clare Garvie, „The Untold Number of People Implicated in Crimes They Didn't Commit Because of Face Recognition | News & Commentary“ (American Civil Liberties Union, 24 June 2020). Prieiga per internetą: <https://www.aclu.org/news/privacy-technology/the-untold-number-of-people-implicated-in-crimes-they-didnt-commit-because-of-face-recognition> (žiūrėta 2022 m. lapkričio 28 d.).

²¹ Monique Mann ir Marcuso Smitho pranešimas „Diskriminacija ir šališkumas VAT“ internetinėje konferencijoje „Veido atpažinimas šiuolaikinėje valstybėje“ (organizavo Lietuvos socialinių mokslo centro Teisės institutas). 1 dalis. Prieiga per internetą: <https://www.youtube.com/watch?v=B-wVfHh7mK4> (žiūrėta 2022 m. spalio 28 d.).

vę paversti kodu. Pavyzdžiui, VAT tamsios odos asmenis atpažįsta mažiau tiksliai, palyginti su šviesios odos asmenimis, ir ši tendencija vis dar išlieka, nepaisant VAT patobulinimų. Teisėsaugos srityje tai gali lemti klaidingus areštus ir įkalinimą²². Taip pat gali būti, kad mašininio mokymosi metu sistemoje atsiranda šališkumas, nes dirbtinis intelektas duomenų rinkinyje atranda tam tikras koreliacijas ar dėsningumus²³.

Pažymėtina ir tai, kad VAT tikslumas dažnai nustatomas išbandant programinę įrangą naudojant aiškias nuotraukas, padarytas esant tinkamam apšvetimui. Tačiau kai VAT taikoma realiame pasaulyje, rezultatams gali turėti įtakos daugybė veiksniai, įskaitant fotoaparato ir vaizdo kokybę, nuotraukos padarymo aplinkybes, veido kryptį, galvos pakreipimą, veido uždengimą ir kt. Net toks pagrindinis veiksnyς kaip šviesa turi įtakos VAT tikslumui: per didelis kiekis šviesos turi įtakos šviesiadžių žmonių veido atvaizdams, o šviesos trūkumas – tamsiaodžių žmonių atvaizdams²⁴.

Socialinė perspektiva susijusi su suvokimu, kad net jei VAT būtų visiškai tikslios, o naudojami mokymo duomenys būtų tolygūs ir nesukeltų šališkumo, praktinis VAT naudojimas, pavyzdžiui, stebimų asmenų sąrašo sudarymas ir VAT dislokavimas konkretiose vietose, vis tiek galėtų sudaryti prielaidas šališkumui ir diskriminacijai²⁵.

Vakarų šalyse rasiniškas šališkumas teisėsaugos institucijose ir per didelis policijos dėmesys kitų nei baltųjų rasės asmenims buvo patvirtintas daugybe tyrimų, buvo atlikta įvairių studijų, susijusių su dažnesniais areštais, kratomis ir sustabdymais²⁶.

²² Pavyzdžiui, žr. „Facial Recognition Tool Led to Mistaken Arrest, Lawyer Says“ (AP NEWS, 2023 m. sausio 2 d.). Prieiga per internetą: <https://apnews.com/article/technology-louisiana-baton-rouge-new-orleans-crime-50e1ea591aed6cf14d248096958dccc4> (žiūrėta 2023 m. kovo 28 d.); Kashmir Hill, „Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match“ *The New York Times* (2020 m. gruodžio 29 d.). Prieiga per internetą: <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html> (žiūrėta 2023 m. kovo 28 d.).

²³ 2014 m. „Amazon“ įdiegė gyvenimo aprašymų atrankos algoritmą, kuris buvo pagrįstas per pastaruoju dešimt metų bendrovės gautų gyvenimo aprašymų vertinimui. Kadangi dauguma gyvenimo aprašymų buvo gauti iš vyrų, ir tai atspindėjo vyrų dominavimą technologijų pramonėje, algoritmas išmoko blogiau vertinti gyvenimo aprašymus, kuriuose buvo tokie terminai kaip „moterų“ (pvz., „moterų šachmatų klubo kapitonė“). „Amazon“ netrukus ištaisė šį šališkumą, tačiau tai atskleidė algoritmo mokymo duomenų svarbą ir galimybę, kad šališkumas atsiranda dėl mašininio mokymosi. Žr. Jeffrey Dastin, „Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women“, *Martin Kirsten (ed.) Ethics of Data and Analytics: Concepts and Cases* (Auerbach Publications 2022).

²⁴ FRA, „Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (žiūrėta 2023 m. kovo 30 d.).

²⁵ Pete Fussey ir Daragh Murray, „Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology“ (University of Essex Human Rights Centre 2019). Prieiga per internetą: <http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf> (žiūrėta 2023 m. kovo 30 d.).

²⁶ Pavyzdžiui, Frank Edwards, Hedwig Lee ir Michael Esposito, „Risk of Being Killed by Police Use of Force in the United States by Age, Race-Ethnicity, and Sex“ (2019) 116 Proceedings of the National Aca-

Buolamwini ir Gebru teigia, kad tamsiaodžiai žmonės dažniau nei kitų rasių asmenys yra fotografuojami veido atpažinimo tikslais²⁷. Australijoje čia buviai yra itin dažnai įtraukiami į baudžiamosios justicijos sistemą²⁸. Panašios tendencijos pastebimos ir Europoje, kur nevietinių gyventojų, ypač tam tikroms rasinėms ir etninėms grupėms priklausančių asmenų, yra sulaikoma neproporcinaliai daug ir jiems skiriamos griežtesnės bausmės²⁹.

Norint tinkamai spręsti VAT šališkumo rizikos problemą, būtina atsižvelgti į abis šias perspektyvas. Nors duomenų perspektyva yra labai svarbi ir kelia pradinius iššūkius, kuriuos reikėtų spręsti nedelsiant, būtina atsižvelgti į socialinę perspektyvą bei į tai, kaip pareigūnai ir viešieji subjektai pasitelkia VAT praktikoje.

2.3. Saviraiškos ir asociacijos laisvės

Veido atpažinimo technologijos taip pat gali turėti didelį poveikį saviraiškos ir asociacijos laisvėms. Šios pasekmės ypač svarbios atsižvelgiant į pasaulinius protesto judėjimus Honkonge, Čilėje, JAV ir kitur. Iš pokalbių su suinteresuotomis šalimis ir literatūros matyti, kad per pastaruosius kelerius metus veido atpažinimo technologijos buvo tiesiogiai naudojamos stebint protestus visame pasaulyje. Pavyzdžiu, buvo išreikštas susirūpinimas, kad Honkonge išsibarsčiusiuose „išmaniuosiuose žibintų stulpuose“ įdiegta veido atpažinimo technologija, leidžianti Kinijos valdžios institucijoms stebeti praeivius. Taip pat manoma, kad JAV teisėsaugos institucijos

demy of Sciences 16793. Prieiga per internetą: <http://www.pnas.org/lookup/doi/10.1073/pnas.1821204116> (žiūrėta 2022 m. vasario 11 d.); Radley Balko, „Opinion. There’s Overwhelming Evidence That the Criminal-Justice System Is Racist. Here’s the Proof.“ (*Washington Post*, 2020). Prieiga per internetą: <https://www.washingtonpost.com/news/opinions/wp/2018/09/18/theres-overwhelming-evidence-that-the-criminal-justice-system-is-racist-heres-the-proof/> (žiūrėta 2023 m. kovo 30 d.).

²⁷ Joy Buolamwini ir Timnit Gebru, „Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification“, *Proceedings of Machine Learning research* (2018). Prieiga per internetą: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (žiūrėta 2022 m. birželio 17 d.).

²⁸ Australian Law Reform Commission, „Over-Representation“ (ALRC, 2018). Prieiga per internetą: <https://www.alrc.gov.au/publication/pathways-to-justice-inquiry-into-the-incarceration-rate-of-aboriginal-and-torres-strait-islander-peoples-alrc-report-133/3-incidence/over-representation/> (žiūrėta 2022 m. lapkričio 23 d.); Amnesty International, „The Overrepresentation Problem: First Nations Kids Are 26 Times More Likely to Be Incarcerated than Their Classmates“ (Amnesty International Australia, 8 September 2022). Prieiga per internetą: <https://www.amnesty.org.au/overrepresentation-explainer-first-nations-kids-are-26-times-more-likely-to-be-incarcerated/> (žiūrėta 2022 m. lapkričio 23 d.).

²⁹ Fair Trials, „Disparities and Discrimination in the European Union’s Criminal Legal Systems“ (*Fair Trials*, 2021). Prieiga per internetą: <https://www.fairtrials.org/articles/publications/disparities-and-discrimination-in-the-european-unions-criminal-legal-systems/> (žiūrėta 2022 m. lapkričio 23 d.).

naudojo veido atpažinimo technologijas, kad identifikuotų dalyvavusius „Black Lives Matters“ protestuose ir stebėtų bei tikrintų minias per 2020 m. protestus, susijusius su George’o Floydo nužudymu. Kaip nurodo žmogaus teisių stebėjimo organizacija „Human Rights Watch“, nuo 2017 m. Rusijos valdžios institucijos visoje šalyje integruoja viešasias stebėjimo sistemas su veido atpažinimo technologijomis ir naudoja šias technologiškai patobulintas sistemas taikių protestų dalyviams nustatyti ir patraukti atsakomybę³⁰. Jungtinės Karalystės nevyriausybinės organizacijos taip pat ypač susirūpinusios dėl veido atpažinimo technologijų naudojimo visoje šalyje siekiant rinkti žvalgybinę informaciją, ypač apie protestus.

Šie pasauliniai pavyzdžiai iliustruoja, kaip policija gali naudoti veido atpažinimo technologijas, kad trukdytų protestų judėjimams, grasindama stebeti minias, tikrinti ir lyginti veidus bei padėti atlkti galimus suėmimus. Stebėjimo viešosiose erdvėse pasekmės yra labai plačios. Šios pasekmės apima ne tik konkrečių asmenų teisę į privatumą, bet ir visos visuomenės galimybes dalyvauti politiniame procese.

2.4. Skaidrumas

Paskutinė šioje ataskaitoje aptariama problema, susijusi su VAT naudojimu, yra skaidrumo trūkumas teisėsaugos institucijoms naudojant VAT. Komentoriai³¹ ir vyriausybinės organizacijos³² nuolat ragina užtikrinti didesnį VAT naudojimo skaidrumą. Daugelyje politinių dokumentų skaidrumas pripažįstamas kaip viena iš pagrindinių dirbtinio intelekto technologijų etinių vertybų ir pagrindinis reikalavimas, susijęs su VAT. Pavyzdžiu, skaidrumo, susijusio su VAT naudojimu teisėsaugos insti-

³⁰ Žmogaus teisių stebėjimo organizacijos „Human Rights Watch“ 2022 m. vasario 10 d. teikimas Žmogaus teisių komitetui dėl Rusijos. Prieiga per internetą: <https://www.hrw.org/news/2022/02/15/-submission-human-rights-watch-russia-human-rights-committee> (žiūrėta 2023 m. kovo 30 d.).

³¹ Pavyzdžiu, Jennifer Lynch, „Face Off: Law Enforcement Use of Face Recognition Technology“ (2020 m. balandžio 20 d.). Prieiga per internetą: <http://dx.doi.org/10.2139/ssrn.3909038>, (žiūrėta 2022 m. lapkričio 23 d.); Benjamin Nober, „A Call for Transparency in Law Enforcement Use of Facial Recognition“ (2020) Northwestern Undergraduate Research Journal. Prieiga per internetą: <https://doi.org/10.21985/n2-nzpa-cv38>; Christopher Jones, „Law Enforcement Use of Facial Recognition“ (2021) *J. L. & Tech.* 777.

³² Pavyzdžiu, NSW Ombudsman, „The new machinery of government: using machine technology in administrative decision-making“ (State of New South Wales 29 November 2021). Prieiga per internetą: www.ombo.nsw.gov.au/Find-a-publication/publications/reports/state-and-local-government/the-new-machinery-of-government-using-machine-technology-in-administrative-decision-making (žiūrėta 2022 m. rugsėjo 15 d.); European Ombudsman, „Report on the meeting between European Ombudsman and European Commission representatives“ (19 November 2021). Prieiga per internetą: www.ombudsman.europa.eu/en/doc/inspection-report/en/149338 (žiūrėta 2022 m. rugsėjo 15 d.).

tucijose, reikalaujama Interpolo/WEF³³, Europos Tarybos³⁴ ir Europos duomenų apsaugos valdybos (EDPB)³⁵ parengtose gairėse. Skaidrumas yra esminis demokratinio valdymo principas, leidžiantis visuomenėi kontroliuoti vyriausybės veiklą ir užtikrinti vyriausybės atskaitomybę. Skaidrumas gali padėti užtikrinti, kad VAT nepagrįstai nepažeistų žmogaus teisių.

Nepaisant to, skaidrumas, susijęs su VAT naudojimu teisėsaugos institucijose, tebéra nepakankamas. Kai kurių šalių policijos institucijos neigia, kad naudoja VAT, kol žiniasklaida neatskleidžia šio naudojimo faktą³⁶. Kitose šalyse pateikiama labai mažai informacijos apie tai, kur, kokiu tikslu ir kaip naudojamos VAT ir kokios apsaugos priemonės taikomos, arba iš viso tokia informacija nepateikiama.

Baudžiamosiose bylose kaltinamieji dažnai nežino, kad jų tapatybei nustatyti buvo naudojamos VAT. Pastaraisiais metais JAV dėl nepakankamo VAT naudojimo skaidrumo prasidėjo teisminiai ginčai. 2019 m. Amerikos pilietinių laisvių sąjunga (ACLU) pateikė ieškinį pagal Informacijos laisvės įstatymą, kuriuo prašoma pateikti dokumentus, susijusius su Federalinio tyrimų biuro (FTB) ir Narkotikų kontrolės tarnybos (DEA) biometrinio stebėjimo ir veido atpažinimo naudojimu. Neseniai organizacija „Surveillance Technology Oversight Project“ (STOP) pateikė ieškinį prieš Metropoliteno transporto tarnybą (MTA) po to, kai agentūra neatskleidė, ar Times'o aikštės transporto mazge įrengtos stebėjimo kameros turi veido atpažinimo funkciją³⁷.

Pagrindinė skaidrumo trūkumo priežastis yra ta, kad skaidrumo principas lieka neigvendinama etine gaire. Be to, nėra aiškių parametru, kaip skaidrumo reikalavimas, susijęs su VAT, turėtų būti įgyvendinamas praktiškai³⁸. Nėra iki galio sutariama,

³³ World Economic Forum (WEF) and others, A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations, Insight Report (Revised), 2022. Prieiga per internetą: https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf.

³⁴ Council of Europe, Guidelines on Facial Recognition, 28 January 2021, T-PD(2020)03rev4. Prieiga per internetą: <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> (žiūrėta 2023 m. kovo 30 d.).

³⁵ European Data Protection Board (EDPB), Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 1, 12 May 2022. Prieiga per internetą: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf (žiūrėta 2023 m. kovo 30 d.).

³⁶ Žr., pvz., Sonia Hickey, Australia: Police accused of lying about use of ineffective facial recognition software, Mondaq, 09 March 2020. Prieiga per internetą: <https://www.mondaq.com/australia/crime/902056/police-accused-of-lying-about-use-of-ineffective-facial-recognition-software> (žiūrėta 2023 m. kovo 30 d.).

³⁷ Hannah Bloch-Wehba, „Visible policing: Technology, Transparency, and Democratic Control“ (2021) 109 Calif. L. Rev. 917, 957.

³⁸ Access Now, „Snapshot Report: Europe’s Approach to AI: How AI Strategy is Evolving“, 2020, p. 3. Prieiga per internetą: <https://www.accessnow.org/cms/assets/uploads/2020/12/Report-Snapshot-Europe-s-approach-to-AI-How-AI-strategy-is-evolving-1.pdf> (žiūrėta 2023 m. kovo 30 d.).

kiek skaidrumo turėtų būti užtikrinama taikant skirtingas VAT priemones (naudojamas autentifikavimo, identifikavimo, klasifikavimo tikslais), pasitelkiant VAT skirtinomis aplinkybėmis ir skirtiniais tikslais. Kai kurios VAT, pavyzdžiui, naudojanos asmenų tapatybei patvirtinti įeinant į patalpas, kelia mažiau susirūpinimo, todėl joms galėtų būti taikomi mažesni skaidrumo standartai. Kiti VAT naudojimo būdai, pavyzdžiui, tikralaikio nuotolinio veido atpažinimo technologijų naudojimas viešose vietose, kelia žmogaus teisių pažeidimo riziką, todėl joms turėtų būti taikomi aukštessni skaidrumo standartai.

3. NAUJAUSIOS POLITINĖS IR TEISINĖS INICIATYVOS VAT SRITYJE

Viešosios institucijos, visuomeninės organizacijos bei mokslininkai visame pasaulyje vis dažniau atkreipia dėmesį į įvairias su VAT naudojimu susijusias problemas. Atsižvelgiant į tai tarptautiniu, regioniniu ir nacionaliniu lygmenimis pradedami rengti įvairūs politiniai pasiūlymai ir teisinės rekomendacijos. Toliau apžvelgsime aktualesnes šios srities iniciatyvas pasaulyje ir Europoje bei pateiksime porą naujų nacionalinių pavyzdžių.

3.1. Pasaulio ekonomikos forumo Politikos programa dėl atsakingo veido atpažinimo technologijų naudojimo

2021 m. spalio mėn. Pasaulio ekonomikos forumas paskelbė dokumentą „Politikos programa dėl atsakingo veido atpažinimo technologijų naudojimo ribų teisėsaugoję“ (angl. *A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations*)³⁹, šis dokumentas buvo peržiūrėtas 2022 m.

Dokumente aptariami VAT naudojimo atvejai ir apibrėžtys, taip pat pateikiamas siūlomų veido atpažinimo naudojimo teisėsaugos tyrimuose principų rinkinys bei savęs vertinimo klausimynas, parengtas siekiant padėti teisėsaugos institucijoms laikytis šių principų. Pateikiamas VAT naudojimo teisėsaugos institucijose principų sąrašas, susijęs su pagarba žmogaus teisėms, būtinumo ir proporcingumo principais, skaidrumu, būtinybe papildomai peržiūrėti VAT išvadas, sistemos veikimu, rizikos mažinimo strategijomis, duomenų bazių legitimumu, vaizdų ir metaduomenų vientisu su poreikiu tinkamai apmokyti VAT naudojančius pareigūnus. Kiekvienas iš šių principų yra išsamiai paaškintas ir detalizuotas.

³⁹ World Economic Forum. A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations. Prieiga per internetą: https://www3.weforum.org/docs/WEF_A-Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf. Nauja dokumento versija paskelbta 2022 m. Prieiga per internetą: https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (žiūrėta 2023 m. kovo 30 d.).

Savęs vertinimo klausimynu siekiama palengvinti šių principų įgyvendinimą, kai VAT priemonės taikomos teisėsaugos praktikoje. Šis dokumentas galėtų būti naudinamas atskaitos taškas formuluojant konkrečioje institucijoje naudojamus klausimynus.

3.2. ES dirbtinio intelekto aktas

2021 m. Europos Komisija parengė pasiūlymą dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas)⁴⁰. Šis dokumentas numato keletą esminių VAT naudojimo principų.

Remiantis Pasiūlymu dėl Dirbtinio intelekto akto, būtų draudžiama viešosiose erdvėse teisėsaugos tikslais realiuoju laiku naudoti nuotolinio biometrinio identifikavimo sistemas, išskyrus tam tikras numatytas išimties. Šios išimties aiškiai įvardijamos, leidžiant VAT naudojimą: (i) vykdant tikslinę konkrečių galimų nusikalstimo aukų, išskaitant dingusius vaikus, paiešką; (ii) siekiant išvengti konkrečios didelės artėjančios grėsmės fizinių asmenų gyvybei ar fizinei saugai arba teroristinio išpuolio; (iii) siekiant išaiškinti asmenis, padariusius nusikalstamą veiką, už kurią atitinkamoje valstybėje narėje jos teisėje nustatyta tvarka baudžiama laisvės atėmimo bausme arba įkalinimu, kurio ilgiausias terminas – bent treji metai, arba asmenis, įtariamus tokios veikos padarymu⁴¹, nustatyti jų buvimo vietą ar tapatybę arba patraukti juos baudžiamojon atsakomybėn. Kai tikralaikio nuotolinio biometrinio tapatybės nustatymo sistemas viešosiose erdvėse teisėsaugos tikslais naudojamos siekiant šių tikslų, taip pat atsižvelgiama į (i) padėties, dėl kurios gali tekti pasinaudoti tokia sistema, pobūdį, visų pirmą žalos, kuri būtų padaryta nenaudojant tokios sistemas, dydį, tikimybę ir mastą; (ii) sistemas naudojimo pasekmes, susijusias su visų atitinkamų asmenų teisėmis ir laisvėmis, visų pirma tų pasekmių rimtumą, tikimybę ir mastą. Taip pat reikalaujama, kad VAT naudojimas būtų būtinas ir proporcinges. Be to, leidimą naudoti VAT kiekvienu konkrečiu atveju turi išduoti teisminė institucija arba nepriklausoma administracinių institucijų; nors išimtiniais atvejais, kai sistemą reikia naudoti nedelsiant, leidimas gali būti suteiktas vėliau⁴².

Dirbtinio intelekto akte taip pat nustatyti griežti skaidrumo ir informacijos apie dirbtinio intelekto naudojimą, išskaitant VAT, atskleidimo naudotojams reikalavimai.

⁴⁰ Pasiūlymas. Europos Parlamento ir Tarybos reglamentas, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimi aktai. COM/2021/206 final.

⁴¹ Siejama su 2002 m. birželio 13 d. Tarybos pagrindų sprendimo 2002/584/TVR dėl Europos arešto ordeirio ir perdavimo tarp valstybių narių tvarkos. OL L 190, 2002 7 18, p. 1; 2(2) straipsniu.

⁴² Pasiūlymo dėl Dirbtinio intelekto akto 5 straipsnis.

Dirbtinio intelekto sistemų naudotojams turi būti pateikiamos išsamios naudojimo instrukcijos. Pažymėtina, kad instrukcijos išduodamos naudotojams, bet ne asmenims, kuriems dirbtinio intelekto sistemos daro poveikį. Akte taip pat nustatyta pareiga informuoti paveiktus asmenis apie dirbtinio intelekto sistemų naudojimą, tačiau joje išsamiai nenurodyta, kiek informacijos turi būti atskleista. Visų pirma fizinius asmenis reikėtų informuoti, kad jie sėveikauja su DI sistema, išskyrus atvejus, kai tai aiškiai matyti iš aplinkybių ir naudojimo konteksto. Be to, fizinius asmenis reikėtų informuoti apie tai, kad jiems taikoma emocijų atpažinimo sistema arba biometrinio kategorizavimo sistema⁴³.

3.3. Europos duomenų apsaugos valdybos gairės dėl VAT teisėsaugos srityje

2022 m. gegužės 12 d. Europos duomenų apsaugos valdyba (EDPB) paskelbė Gairės 05/2022 dėl veido atpažinimo technologijos naudojimo teisėsaugos srityje⁴⁴. Šios gairės skirtos ES ir nacionalinio lygmens teisės aktų leidėjams, taip pat teisėsaugos institucijoms ir jų pareigūnams, diegiantiems ir naudojantiems VAT sistemas.

Gairėmis siekiama informuoti apie tam tikras VAT savybes ir taikytinus ES teisės aktus teisėsaugos kontekste (plačiau aptariant ES Teisėsaugos direktyvą⁴⁵). Be to, jose pateikiama priemonė, padedanti pirmą kartą klasifikuoti konkretaus VAT naudojimo atvejo jautrumą. Gairėse taip pat pateikiamos praktinės rekomendacijos teisėsaugos institucijoms, norinčioms įsigyti ir naudoti VAT sistemą. Naudinga ir tai, kad gairėse apžvelgiami keli tipiniai naudojimo atvejai ir aptariami būtinumo ir proporcijumo testai.

⁴³ Pasiūlymo dėl Dirbtinio intelekto akto 70 konstatuojamoji dalis.

⁴⁴ European Data Protection Board. Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement. Prieiga per internetą: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frlawenforcement_en_1.pdf (žiūrėta 2023 m. kovo 30 d.).

⁴⁵ 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. OL L 119, 2016 5 4, p. 89–131.

3.4. Europos Tarybos gairės dėl VAT naudojimo

2021 m. Europos Tarybos konsultacinis komitetas dėl 108 konvencijos (Konvenčija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu) paskelbė Gaires dėl veido atpažinimo technologijų naudojimo⁴⁶. Gairėse pateikiamos rekomendacijos, skirtos užtikrinti etišką ir teisėtą šių technologijų naudojimą.

Dokumente pateikiami atskiri gairių rinkiniai, skirti teisės aktų leidėjams ir sprendimų priėmėjams, veido atpažinimo sistemų kūrėjams, gamintojams, paslaugų teikėjams, subjektams, naudojantiems veido atpažinimo technologijas, bei atskiras skyrius apie duomenų subjektų teises. Šių gairių taikymas turėtų padėti užtikrinti, kad VAT nedarytų neigiamo poveikio asmens orumui, žmogaus teisėms ir pagrindinėms laisvėms, įskaitant teisę į asmens duomenų apsaugą. Dokumente aptariamas VAT teisėtumas, būtinas priežiūros institucijų dalyvavimas, sertifikavimas, informuotumo didinimas, duomenų ir algoritmu kokybė, naudojamų priemonių patikimumas, atskaitomybė, duomenų tvarkymo teisėtumas, duomenų saugumas, etinė sistema.

3.5. Iniciatyvos Jungtinėje Karalystėje

Praeitais metais, Jungtinėje Karalystėje atlikus nepriklausomą teisės aktų peržiūrą, padaryta išvada, kad šaliai skubiai reikalangi nauji įstatymai, reglamentuojantys biometrinį technologijų naudojimą, ir vyriausybė buvo paraginta parengti reikalingus teisės aktus⁴⁷. Tarp dešimties pateiktų teisinės peržiūros rekomendacijų yra ir tokia: sustabdyti tikralaikių nuotolinio veido atpažinimo technologijų naudojimą viešojoje erdvėje, kol bus sukurtas teisiškai privalomas tokį naudojimą reglamentuojantis praktikos kodeksas ir kol bus priimti platesnio masto, technologiškai neutralūs teisės aktai, kuriais būtų sukurta įstatyminė sistema, reglamentuojanti biometrinį duomenų naudojimą⁴⁸.

Škotijoje 2022 m. lapkričio mėn. paskelbtas Biometrinį duomenų gavimo, naujodimo, saugojimo ir sunaikinimo teisingumo ir bendruomenės saugumo tikslais

⁴⁶ Council of Europe. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108). Guidelines on facial recognition (2021). Prieiga per internetą: <https://edoc.coe.int/en/artificial-intelligence/9753-guidelines-on-facial-recognition.html> (žiūrėta 2023 m. kovo 31 d.).

⁴⁷ UK urgently needs new laws on use of biometrics, warns review. June 29, 2022. Prieiga per internetą: <https://techcrunch.com/2022/06/28/uk-biometrics-legal-review/> (žiūrėta 2023 m. kovo 31 d.).

⁴⁸ Ibid.

Škotijoje praktikos kodeksas⁴⁹. Šiuo kodeksu siekiama spręsti minimas problemas nustatant 12 principų ir etinių aspektų, kuriuose išsamiai aprašoma, kaip biometriniai duomenys gali būti įgyjami, saugomi, naudojami ir naikinami baudžiamojo teisingumo srityje ir policijos veikloje. Šie principai apima lygybę, teisėtą valdžią, etiką, privatumą, pagarbą žmogaus teisėms ir mokslo bei technologijų pažangos skatinimą.

3.6. Iniciatyvos Naujojoje Zelandijoje ir Australijoje

2020 m. rugsėjį Naujosios Zelandijos policija paskelbė naują politiką, skirtą modernių technologijų naudojimui⁵⁰. Politikoje pateikiamas gairės policijos darbuotojams, kuriems suteikiama galimybė naudoti ar išbandyti naujas technologijas, ir nurodomi veiksmai, kurių reikia imtis prieš išbandant ar diegiant tokias technologijas. Ji taip pat taikoma tais atvejais, kai esama technologija papildoma naujomis funkcijomis. Šia politika įdiegtas naujas dviejų pakopų valdymo ir priežiūros procesas. 2021 m. buvo atlirkas tolesnis darbas, peržiūrėta politika ir parengta Naujujų technologijų sistema. Daug dėmesio skiriama policijos veiklos sąžiningumo ir skaidrumo principams, visuomenės saugumui bei teisei į privatumą⁵¹.

Australijoje Australijos žmogaus technologijų institutas (angl. *Australian Human Technology Institute*), vadovaujamas buvusio Australijos žmogaus teisių komisaro Edo Santow, parengė ataskaitą „Veido atpažinimo technologija – pavyzdinio įstatymo link“⁵². Ataskaitoje siūloma rizika grindžiama sistema, pagal kurią VAT kūrėjai ir organizacijos, siekiančios naudoti VAT, privalėtų atliki VAT galimos žalos, išskaitant galimą riziką žmogaus teisėms, vertinimą. Šis „VAT poveikio vertinimas“ būtų registruojamas, viešai prieinamas ir jį galėtų užginčiti reguliavimo institucija arba suinteresuotosios šalys. Atliekant VAT poveikio vertinimą būtų atsižvelgiama į įvairius siū-

⁴⁹ Code of Practice. On the acquisition, use, retention and disposal of biometric data for justice and community safety purposes in Scotland. Prieiga per internetą: <https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-paper/2018/07/consultation-enhanced-overight-biometric-data-justice-community-safety-purposes/documents/00538315-pdf/00538315-pdf/govscot%2-53Adocument/?inline=true> (žiūrėta 2023 m. kovo 31 d.).

⁵⁰ New Zealand Police. Trial or adoption of new policing technology - Police Manual chapter. Prieiga per internetą: <https://www.police.govt.nz/about-us/publication/trial-or-adoption-new-policing-technology-police-manual-chapter> (žiūrėta 2023 m. kovo 31 d.).

⁵¹ *Ibid.*

⁵² Davis, N., Perry, L. & Santow, E. (2022) Facial Recognition Technology: Towards a model law, Human Technology Institute, The University of Technology Sydney. Prieiga per internetą: <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20law%20report.pdf> (žiūrėta 2023 m. kovo 31 d.).

lomo VAT naudojimo veiksnius, įskaitant kontekstą, funkcionalumą, veikimą ir tai, ar asmenys turi galimybę duoti laisvą ir informuotą sutikimą. VAT kūrėjas ar naudojantis subjektas taip pat turėtų apsvarstyti, ar pasitelkus technologijas gaunami rezultatai, kuriais remiantis priimami teisinį ar panašų reikšmingą poveikį turintys sprendimai, bei apsvarstyti, ar tokie sprendimai yra visiškai ar iš dalies automatizuoti. Šiuo atžvilgiu remiamasi Europos bendrajame duomenų apsaugos reglamente⁵³ nustatytomis sąvokomis.

⁵³ Facial recognition technology: a model law. 4 October 2022. Prieiga per internetą: <https://www.corts.com.au/insights/facial-recognition-technology-a-model-law> (žiūrėta 2023 m. kovo 31 d.).

4. REKOMENDACIJOS

Atsižvelgdami į aptartas VAT keliamas rizikas ir į naujausius tarptautinius dokumentus, siūlančius, kaip valdyti šias rizikas teisėsaugos kontekste, parengėme šias rekomendacijas Lietuvos valdžios ir teisėsaugos institucijoms, kurios padėtų užtikrinti etišką ir teisętą veido atpažinimo technologijų naudojimą teisėsaugos kontekste.

4.1. Aiškus ir konkretus teisinis pagrindas

1. Be bendruųjų įstatymų, reglamentuojančių asmens duomenų naudojimą (įskaitant biometrinius duomenis), turėtų būti priimami specialūs aktai, reguliuojantys VAT naudojimą teisėsaugos kontekste.

2. Sie teisės aktai turėtų apimti bent šiuos svarbius klausimus:

- kokiose situacijose teisėsaugos institucijos galėtų naudoti VAT ir kokiais tikslais; kokių nusikaltimų ar tyrimų kategorijų atveju VAT naudojimas yra leidžiamas ir (arba) teisėtas;
- kokiems teisėsaugos institucijų padaliniams ir skyriams leidžiama naudoti VAT ir kokios procedūros jie turėtų laikytis, pvz., kokiai atvejais padalinui ar skyriui reikalingas leidimas, iš kokio subjekto ir kokia tvarka tokis leidimas naudoti VAT turėtų būti gautas;
- kaip, taikant VAT, atrenkami technologijomis analizuojami atvaizdai ir kokios duomenų bazės gali būti naudojamos bei kokiai atvejais; kada ir kokiais kriterijais remiantis vaizdai turi būti pašalinti iš rinkinio arba duomenų bazės;
- teisės aktuose turėtų būti reikalaujama, kad teisėsaugos institucijos, siekiančios naudoti tikralaikio nuotolinio biometrinio tapatybės nustatymo technologijas, įprastai turėtų gauti atsakingų institucijų *ex ante* leidimą naudoti VAT konkrečiam atvejui. Išimtiniais atvejais, pvz., esant kritinei situacijai, leidimą naudoti VAT galėtų suteikti vadovybė. Tokiu atveju vadovybė turėtų informuoti nepriklausomą instituciją apie priimtą sprendimą ir jį pagrįsti per iš anksto nustatyta laikotarpį

4.2. Pagarba žmogaus teisėms

1. Aukščiau aptarti teisės aktai turėtų būti grindžiami pagarba pagrindinėms žmogaus teisėms, ypač teise į žmogaus orumą, teise į privatų gyvenimą, asmens duomenų apsaugą, teise į lygybę ir nediskriminavimą, saviraiškos, asociacijų ir taikių susirinkimų laisvėmis, vaikų ir vyresnio amžiaus žmonių teisėmis, neigalių asmenų teisėmis, migrantų teisėmis ir įtariamųjų, sulaikytųjų ar įkalinamujų asmenų procesinėmis teisėmis, kaip numatyta tarptautiniuose ir nacionaliniuose teisės aktuose.

2. Kaip numatoma nacionaliniuose ir tarptautinės bei ES teisės žmogaus teisių dokumentuose, šios teisės gali būti ribojamos tik tada, kai tai yra būtina ir proporcinga siekiant užtikrinti visuomenės interesus (pvz., visuomenės saugumą).

3. Siekiant įvertinti, kaip siūlomas VAT naudojimas paveiks žmogaus teises ir ar šis poveikis yra būtinas ir proporcingas, atsakinga institucija turėtų atligli VAT poveikio teisei į privatumą ir, pageidautina, platesnio masto poveikio žmogaus teisėms vertinimą.

4. Siekiant apriboti nereikalingą kišimąsi į žmogaus teises, VAT turėtų būti naudojamos tik atliekant baudžiamajį tyrimą, pavyzdžiui, siekiant nustatyti įtariamujų tapatybę, rasti dingusius asmenis, ieškomus asmenis ir aukas. VAT galėtų būti naudojamos siekiant užkirsti kelią konkretių numatomam nusikaltimui, tačiau jos neturėtų būti naudojamos bendriems nusikaltimų prevencijos tikslams.

5. Vertėtų nustatyti konkretias, išsamesnes taisykles, susijusias su didžiausios rizikos VAT, pavyzdžiui, VAT, naudojamomis tapatybės nustatymo tikslais, ypač tikralaikiam nuotliniam tapatybės nustatymui viešosiose erdvėse. Veido atvaizdų rinkimas iš viešųjų ir viešai prieinamų erdvinių tikralaikio tapatybės nustatymo tikslais turėtų būti draudžiamas, išskyrus atvejus, kai teisės aktai numato konkretias ir ribotas išimtis. Naudoti VAT tikralaikiam nuotliniam tapatybės nustatymui viešosiose erdvėse galėtų būti leidžiama tik konkretiai įstatymų apibrėžtais atvejais, ribotoje teritorijoje ir nustatyta laikotarpi.

6. VAT neturėtų būti naudojamos jokiais kitais tikslais, išskyrus biometrinį tapatybės nustatymo ir (arba) tikrinimo tikslais ar asmens atpažinimui. Neturėtų būti leidžiama naudoti VAT siekiant nustatyti etninę kilmę, lytį, amžių, emocijas, nuomonę, sveikatos būklę, religiją ir seksualinę orientaciją, taip pat naudoti VAT prognozavimui.

4.3. Kokybės užtikrinimas

1. Kokybės užtikrinimas prieš pradedant naudoti VAT turėtų remtis šiais principais:

- prieš pradėdamos naudoti VAT, teisėsaugos institucijos turėtų imtis prie-monių užtikrinti, kad veido atpažinimo sistemos atitiktų naujausius nacio-nalinius ir regioninius standartus ir kad jų kokybę ir tikslumą patvirtintų akredituotos institucijos, vadovaudamosi atitinkamomis sertifikavimo pro-cedūromis (jei tokios sertifikavimo procedūros egzistuoja);
- teisėsaugos institucijos turėtų reikalauti, kad VAT pardavėjai atliktų išsa-mius ir nepriklasomus savo algoritmų bandymus, atliekamus pagal atitin-kamus bandymų standartus (laboratoriniai bandymai ir, jei įmanoma, ban-dymai realiojoje aplinkoje, pvz., lauke, viešosiose erdvėse), ir atrinktų tiekė-jus, kurie gali įrodyti, kad algoritmo veiksmingumas atitinka standartus.

2. Kokybės užtikrinimas naudojant VAT turėtų remtis šiais principais:

- siekdamos nuolat stebėti ir gerinti procesų kokybę ir sistemos veikimą, teisė-saugos institucijos, technologijų diegėjai ir technologijų tiekėjai turėtų nus-tatyti vidaus kontrolę, taikomą per visą sistemos gyvavimo ciklą;
- per visą VAT sistemos gyvavimo ciklą turėtų būti reguliariai atliekamas tech-ninis auditas, kad būtų užtikrinta, jog VAT atitinka reikalaujamus techni-nius standartus ir specifikacijas.

4.4. Nuolatinė priežiūra ir atskaitomybė

1. Prieš perduodant bet kokį teigiamą pasitelkus VAT gautą rezultatą tyréjų gru-pei, šis rezultatas turėtų būti papildomai peržiūrėtas žmogaus eksperto. Pateiktas galutinis rezultatas visada turėtų būti grindžiamas bendru sutarimu, o pirmenybė turėtų būti teikiama konservatyviausiai išvadai.

2. Teisėsaugos institucijos veikla naudojant VAT turėtų būti prižiūrima institu-cijos, turinčios įgaliojimus kontroliuoti VAT naudojimą teisėsaugos institucijų veik-loje. Ši institucija turėtų reguliariai tikrinti, kaip teisėsaugos institucijos naudoja VAT, ar jos tinkamai atsižvelgia į žmogaus teises ir teisinius reikalavimus, bei teiki rekomendacijas, kaip būtų galima pagerinti teisinį reguliavimą ir jo laikymąsi.

3. Kiekvienas asmuo turėtų turėti teisę į veiksmingą teisinę gynybą nepriklasuso-me ir nešališkoje administracinėje ar teisminėje institucijoje dėl teisėsaugos insti-tucijų veiksmų, naudojant VAT. Teisėsaugos institucija turėtų užtikrinti, kad piliečiai galėtų pateikti skundą priežiūros institucijai arba kreiptis į ją dėl žalos atlyginimo.

4. Turėtų būti aiškiai apibrėžta atsakomybė už VAT konkretaus panaudojimo rezultatus. Teisėsaugos institucija niekada neturėtų naudoti veido atpažinimo sistemos išvadą, jei jų nepatikrino teisėsaugos institucijos ekspertas, turintis tinkamą kompetenciją veidų atpažinimo ir VAT naudojimo srityje.

4.5. Skaidrumas ir visuomenės informuotumo didinimas

1. Asmuo, kurio tapatybė nustatyta naudojant veido atpažinimo sistemą, turėtų būti apie tai informuotas, ypač jei jis vėliau sulaikomas, pristatomas kaip liudytojas ar atlieka bet kokį procesinį vaidmenį.

2. Teisėsaugos institucijos turėtų užtikrinti, kad VAT naudojimas būtų skaidrus. Jos turėtų visuomenei pateikti bent šią informaciją:

- informaciją, kad teisėsaugos srityje VAT yra naudojamos;
- paaiškinimą, kokiais tikslais technologijos naudojamos (pvz., įtariamiesiems nustatyti, dingusių asmenų paieškai, aukų tapatybei nustatyti *etc.*);
- paaiškinimą, kaip atrenkami VAT analizuotini atvaizdai (*angl. probe images*), ar jie saugomi ir, jei taip, kiek laiko;
- informaciją, kokios duomenų bazės naudojamos atvaizdų atitikimo analizės procese (kiek atvaizdų jose yra; kokie yra šių atvaizdų šaltiniai);
- informaciją, kokie teisėsaugos institucijos skyriai gali atlkti paiešką veido atpažinimo sistemoje ir peržiūrėti paieškos rezultatus;
- informaciją apie VAT naudojimą reglamentuojančius teisės aktus. Pageidautina pateikti vartotojui patogią taisyklių santrauką ir suteikti galimybę susipažinti su visais VAT naudojimą reglamentuojančiais teisės aktais;
- informaciją apie tai, kokį poveikį VAT naudojimas gali turėti žmogaus teisėms ir kokios buvo įdiegtos neigiamo poveikio mažinimo strategijos, išskaitant poveikio žmogaus teisėms vertinimus;
- informaciją apie įdiegtas kokybės užtikrinimo sistemas, išskaitant technologijos pardavėjo atliktą VAT veiksmingumo vertinimų rezultatus;
- informaciją apie priežiūros ir atskaitomybės priemones, išskaitant informaciją apie tai, kaip ir kur asmenys gali pateikti skundą dėl VAT naudojimo.

Visuomenei teikiama informacija turėtų būti glausta, lengvai prieinama, suprantama ir pateikiama aiškia bei paprasta kalba.

3. Teisėsaugos institucijos turėtų saugoti visus dokumentus, susijusius su naudojamomis VAT technologijomis, fiksuoti jų naudojimą ir sudaryti galimybę su šiais dokumentais susipažinti vidaus ar išorės audito ir (arba) priežiūros institucijoms.

4. Teisėsaugos institucijos turėtų aktyviai įsitraukti į viešą dialogą apie VAT galimybes ir rizikas ir prisdėti prie visuomenės informuotumo šiaisiai klausimais didinimo.

4.6. Profesinis mokymas

1. Teisėsaugos pareigūnai turėtų būti tinkamai apmokyti naudotis VAT. VAT naudojančių asmenų įgūdžiai yra labai svarbūs ir būtini, kad tapatybės nustatymo procesas būtų kuo tikslesnis.

2. Visi teisėsaugos institucijų darbuotojai, ypač vadovybė, turėtų galimybę nuolat plėsti žinias ir kelti kvalifikaciją VAT srityje, kad būtų tinkamai informuoti apie naudojamą sistemą galimybes, ribas ir rizikas.

BIBLIOGRAFIJA

Teisés aktais

2002 m. birželio 13 d. Tarybos pagrindųsprendimo 2002/584/TVR dėl Europosarešto orderio ir perdavimo tarp valstybių narių tvarkos. OL L 190, 2002 7 18, p. 1.

2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokiau duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. OL L 119, 2016 5 4, p. 89–131.

2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokiau duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119, 4.5.2016, p. 1–88.

2017 m. lapkričio 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2226, kuriuo sukuriama atvykimo ir išvykimo sistema (AIS), kurioje registruojami trečiųjų šalių piliečių, kertančių valstybių narių išorės sienas, atvykimo ir išvykimo bei atsisakymo leisti jiems atvykti duomenys, nustatomos prieigos prie AIS teisėsaugos tikslais sąlygos ir iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir reglamentai (EB) Nr. 767/2008 ir (ES) Nr. 1077/2011. OJ L 327, 9.12.2017, p. 20–82.

Europos Komisija „Baltoji knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“. COM(2020) 65 final. Prieiga per internetą: https://op.europa.eu/lt/publication_detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1 (žiūrėta 2023 m. kovo 29 d.).

Pasiūlymas. Europos Parlamento ir Tarybos reglamentas, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisékūros procedūra priimti aktais. COM/2021/206 final.

Tarptautinių ir ES institucijų dokumentai (privalomos teisinės galios neturintys teisés aktais)

Council of Europe, Guidelines on Facial Recognition, 28 January 2021, T-PD(2020)03rev4

Prieiga per internetą: <https://rm.coe.int/guidelines-on-facial-recognition/1680a134f3> (žiūrėta 2023 m. kovo 30 d.).

European Data Protection Board (EDPB), Guidelines 05/2022 on the use of facial recognition technology in the area of law enforcement, version 1, 12 May 2022. Prieiga per internetą: https://edpb.europa.eu/system/files/2022-05/edpb-guidelines_202205_frtlawenforcement_en_1.pdf (žiūrėta 2023 m. kovo 30 d.).

World Economic Forum (WEF). A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations, Insight Report (Revised), 2022. Prieiga per internetą: https://www3.weforum.org/docs/WEF_Facial_Recognition_for_Law_Enforcement_Investigations_2022.pdf (žiūrėta 2023 m. kovo 30 d.).

World Economic Forum. A Policy Framework for Responsible Limits on Facial Recognition Use Case: Law Enforcement Investigations. Prieiga per internetą: https://www3.weforum.org/-docs/WEF_A_Policy_Framework_for_Responsible_Limits_on_Facial_Recognition_2021.pdf (žiūrėta 2023 m. kovo 30 d.).

Mokslinė literatūra

Benjamin Nober, „A Call for Transparency in Law Enforcement Use of Facial Recognition“ (2020) Northwestern Undergraduate Research Journal. Prieiga per internetą: <https://doi.org/10.21985/n2-nzpa-cv38>.

Christopher Jones, „Law Enforcement Use of Facial Recognition“ (2021) J. L. & Tech. 777.

Dean Knox, Will Lowe ir Jonathan Mummolo, „Administrative Records Mask Racially Biased Policing“ (2020) 114 American Political Science Review 619. Prieiga per internetą: https://www.cambridge.org/core/product/identifier/S0003055420000039/type/journal_article (žiūrėta 2022 m. lapkričio 16 d.).

Frank Edwards, Hedwig Lee ir Michael Esposito, „Risk of Being Killed by Police Use of Force in the United States by Age, Race-Ethnicity, and Sex“ (2019) 116 Proceedings of the National Academy of Sciences 16793. Prieiga per internetą: <http://www.pnas.org/lookup/doi/10.1073/pnas.1821204116> (žiūrėta 2022 m. vasario 11 d.).

Hannah Bloch-Wehba, „Visible policing: Technology, Transparency, and Democratic Control“ (2021) 109 Calif. L. Rev. 917, 957.

Joy Buolamwini ir Timnit Gebru, „Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification“, Proceedings of Machine Learning research (2018). Prieiga per internetą: <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> (žiūrėta 2022 m. birželio 17 d.).

Kristina Murphy ir kiti, „Police Bias, Social Identity, and Minority Groups: A Social Psychological Understanding of Cooperation with Police“ (2018) 35 Justice Quarterly 1105. Prieiga per internetą: <https://doi.org/10.1080/07418825.2017.1357742> (žiūrėta 2022 m. lapkričio 16 d.).

Lois James, „The Stability of Implicit Racial Bias in Police Officers“ (2018) 21 Police Quarterly 30. Prieiga per internetą: <https://doi.org/10.1177/109861111732974> (žiūrėta 2022 m. lapkričio 16 d.).

Lynch, Jennifer, „Face Off: Law Enforcement Use of Face Recognition Technology“ (2020 m. balandžio 20 d.). Prieiga per internetą: <http://dx.doi.org/10.2139/ssm.3909038>, 27 (žiūrėta 2022 m. lapkričio 23 d.).

Marcus Smith, Monique Mann ir Gregor Urbas, Biometrics, Crime and Security (Taylor & Francis 2018).

P Jeffrey Brantingham, Matthew Valasik ir George O Mohler, „Does Predictive Policing Lead to Biased Arrests? Results From a Randomized Controlled Trial“ (2018) 5 Statistics and Public Policy 1 Prieiga per internetą: <https://doi.org/10.1080/2330443X.2018.1438940> (žiūrėta 2022 m. lapkričio 16 d.).

Pete Fussey ir Daragh Murray, „Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology“ (University of Essex Human Rights Centre 2019). Prieiga per internetą: <http://repository.essex.ac.uk/24946/1/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report-2.pdf> (žiūrėta 2023 m. kovo 30 d.).

Yilun Wang ir Michal Kosinski, „Deep Neural Networks Are More Accurate than Humans at Detecting Sexual Orientation from Facial Images“ (2018) 114 Journal of Personality and Social Psychology 246. Prieiga per internetą: <http://doi.apa.org/getdoi.cfm?doi=10.1037/pspa0000098> (žiūrėta 2023 m. sausio 21 d.).

Kita literatūra

„Home | IBorderCtrl“. Prieiga per internetą: <https://www.iborderctrl.eu/> (žiūrėta 2023 m. vasario 6 d.).

„TechDispatch #1/2021 - Facial Emotion Recognition | European Data Protection Supervisor“ (1 February 2023). Prieiga per internetą: <https://edps.europa.eu/data-protection/our-work/publications/techdispatch/techdispatch-12021-facial-emotion-recognition> (žiūrėta 2023 m. vasario 6 d.).

„Facial Recognition Tool Led to Mistaken Arrest, Lawyer Says“ (APNEWS, 2023 m. sausio 2 d.). Prieiga per internetą: <https://apnews.com/article/technology-louisiana-baton-rouge-new-orleans-crime-50e1ea591aed6cf14d248096958dccc4> (žiūrėta 2023 m. kovo 28 d.).

Access Now, „Snapshot Report: Europe’s Approach to AI: How AI Strategy is Evolving“, 2020. Prieiga per internetą: <https://www.accessnow.org/cms/assets/uploads/2020/12/Report-Snapshot-Europe-s-approach-to-AI-How-AI-strategy-is-evolving-1.pdf> (žiūrėta 2023 m. kovo 30 d.).

Amnesty International, „The Overrepresentation Problem: First Nations Kids Are 26 Times More Likely to Be Incarcerated than Their Classmates“ (*Amnesty International Australia*,

8 September 2022). Prieiga per internetą: <https://www.amnesty.org.au/overrepresentation-explainer-first-nations-kids-are-26-times-more-likely-to-be-incarcerated/> (žiūrėta 2022 m. lapkričio 23 d.).

Article 19.org, „Emotion Recognition Technology Report“ (ARTICLE 19, 2021). Prieiga per internetą: <https://www.article19.org/emotion-recognition-technology-report/> (žiūrėta 2022 m. lapkričio 22 d.).

Australian Law Reform Commission, „Over-Representation“ (ALRC, 2018). Prieiga per internetą: <https://www.alrc.gov.au/publication/pathways-to-justice-inquiry-into-the-incarceration-rate-of-aboriginal-and-torres-strait-islander-peoples-alrc-report-133/3-incidence-over-representation/> (žiūrėta 2022 m. lapkričio 23 d.).

Code of Practice. On the acquisition, use, retention and disposal of biometric data for justice and community safety purposes in Scotland. Prieiga per internetą: <https://www.gov.scot/binaries/content/documents/govscot/publications/consultation-paper/2018/07/consultation-enhanced-oversight-biometric-data-justice-community-safety-purposes/documents/00538315-pdf/00538315-pdf/govscot%3Adocument/?inline=true> (žiūrėta 2023 m. kovo 31 d.).

Davis, N., Perry, L. & Santow, E. (2022) Facial Recognition Technology: Towards a model law, Human Technology Institute, The University of Technology Sydney. Prieiga per internetą: <https://www.uts.edu.au/sites/default/files/2022-09/Facial%20recognition%20model%20-law%20report.pdf> (žiūrėta 2023 m. kovo 31 d.).

European Ombudsman, „Report on the meeting between European Ombudsman and European Commission representatives“ (19 November 2021). Prieiga per internetą: www.ombudsman.europa.eu/en/doc/inspection-report/en/149338 (žiūrėta 2022 m. rugėjo 15 d.).

Facial recognition technology: a model law. 4 October 2022. Prieiga per internetą: <https://www.corrs.com.au/insights/facial-recognition-technology-a-model-law> (žiūrėta 2023 m. kovo 31 d.).

Fair Trials, „Disparities and Discrimination in the European Union’s Criminal Legal Systems“ (Fair Trials, 2021). Prieiga per internetą: <https://www.fairtrials.org/articles/publications-disparities-and-discrimination-in-the-european-unions-criminal-legal-systems/> (žiūrėta 2022 m. lapkričio 23 d.).

FRA, „Facial Recognition Technology: Fundamental Rights Considerations in the Context of Law Enforcement“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf (žiūrėta 2023 m. kovo 30 d.).

FRA, „Under Watchful Eyes: Biometrics, EU IT Systems and Fundamental Rights“. Prieiga per internetą: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-biometrics-fundamental-rights-eu_en.pdf (žiūrėta 2023 m. kovo 30 d.).

Clare Garvie, „The Untold Number of People Implicated in Crimes They Didn’t Commit Because of Face Recognition | News & Commentary“ (*American Civil Liberties Union*, 24 June 2020). Prieiga per internetą: <https://www.aclu.org/news/privacy-technology/the-untold-number-of-people-implicated-in-crimes-they-didnt-commit-because-of-face-recognition> (žiūrėta 2022 m. lapkričio 28 d.).

Greens Efa, „Facial Recognition in European Cities - Read Our New Study“ (*Greens/EFA*, 22 October 2021). Prieiga per internetą: <https://www.greens-efa.eu/opinions/facial-recognition-in-european-cities-what-you-should-know-about-biometric-mass-surveillance/> (žiūrėta 2023 m. vasario 6 d.).

Jeffrey Dastin, „Amazon Scraps Secret AI Recruiting Tool That Showed Bias against Women“ (*Martin Kirsten (ed.) Ethics of Data and Analytics: Concepts and Cases* (Auerbach Publications 2022)).

Kashmir Hill, „Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match“ (*The New York Times* (2020 m. gruodžio 29 d.). Prieiga per internetą: <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html> (žiūrėta 2023 m. kovo 28 d.).

Monique Mann ir Marcuso Smitho pranešimas „Diskriminacija ir šališumas VAT“ interne tinėje konferencijoje „Veido atpažinimas šiuolaikinėje valstybėje“ (organizavo Lietuvos socialinių mokslų centro Teisės institutas). 1 dalis. Prieiga per internetą: <https://www.youtube.com/watch?v=B-wVfHh7mK4> (žiūrėta 2022 m. spalio 28 d.).

New Zealand Police. Trial or adoption of new policing technology - Police Manual chapter. Prieiga per internetą: <https://www.police.govt.nz/about-us/publication/trial-or-adoption-new-policing-technology-police-manual-chapter> (žiūrėta 2023 m. kovo 31 d.).

Nicholas Fletcher, „Lincs Police to Trial New CCTV Tech That Can Tell If You’re in a Mood“ (*LincolnshireLive*, 17 August 2020). Prieiga per internetą: <https://www.lincolnshirelive.co.uk/news/local-news/new-lincolnshire-police-cctv-technology-4431274> (žiūrėta 2022 m. lapkričio 21 d.).

NSW Ombudsman, „The new machinery of government: using machine technology in administrative decision-making“ (State of New South Wales 29 November 2021). Prieiga per internetą: <https://www.ombo.nsw.gov.au/Find-a-publication/publications/reports/state-and-local-government/the-new-machinery-of-government-using-machine-technology-in-administrative-decision-making> (žiūrėta 2022 m. rugėjo 15 d.).

Radley Balko, „Opinion. There’s Overwhelming Evidence That the Criminal-Justice System Is Racist. Here’s the Proof.“ (*Washington Post*, 2020). Prieiga per internetą: <https://www.washingtonpost.com/news/opinions/wp/2018/09/18/theres-overwhelming-evidence-that-the-criminal-justice-system-is-racist-heres-the-proof/> (žiūrėta 2023 m. kovo 30 d.).

Sonia Hickey, Australia: Police accused of lying about use of ineffective facial recognition software, Mondaq, 09 March 2020. Prieiga per internetą: <https://www.mondaq.com/-australia/crime/902056/police-accused-of-lying-about-use-of-ineffective-facial-recognition-software> (žiūrėta 2023 m. kovo 30 d.).

UK urgently needs new laws on use of biometrics, warns review. June 29, 2022. Prieiga per internetą: <https://techcrunch.com/2022/06/28/uk-biometrics-legal-review> (žiūrėta 2023 m. kovo 31 d.).

Žmogaus teisių stebėjimo organizacijos „Human Rights Watch“ 2022 m. vasario 10 d. teikimas Žmogaus teisių komitetui dėl Rusijos. Prieiga per internetą: <https://www.hrw.org/news/2022/02/15/submission-human-rights-watch-russia-human-rights-committee> (žiūrėta 2023 m. kovo 30 d.).