Vilnius University Press

Contents lists available at Vilnius University Press

Politologija
2022/2, vol. 106, pp. 131–164

ISSN 1392-1681 eISSN 2424-6034
DOI: https://doi.org/10.15388/Polit.2022.106.4

Vizualioji kontrolė šiandienos visuomenėse: veidų ir emocijų (ne)atpažinimas

Skaidra Trilupaitytė

Lietuvos kultūros tyrimų institutas, vyresnioji mokslo darbuotoja
El. paštas: s.trilupaityte@gmail.com

Santrauka. Pasitelkiant sekimo kapitalizmo kritikos teorinę prieigą ir naudojantis viešojo diskurso (žiniasklaidos) medžiaga apie veidų atpažinimo (VA) technologiją, tekste analizuojama vizualioji kontrolė šiandienos visuomenėse. Apžvelgiamos staigios VA galimybių plėtros pasaulyje aplinkybės ir pastangos užkardyti šią „pačią pavojingiausią technologiją“. Taip pat kvestionuojamos „tobulą“ matematinį žmogaus pažinimą įgalinančios besąlygiško technologijų naudingumo (angl. *techno solutionism*) nuostatos. Šiuo metu pasaulyje nesutariama dėl VA technologijos reguliavimo terpės – skirtingose šalyse, valstijose ar miestuose biometrinių duomenų apsauga traktuojama nevienodai, o viešojoje erdvėje su VA susiję precedentai ir teisiniai nuogąstavimai susipina. Vis dėlto galima minėti žiniasklaidos diskursuose išryškėjančius tipiškus naratyvus; jie akcentuojami pasirenkant tris skirtingus pavyzdžius arba prieigas. Tai – 1. rūpestis dėl žmogaus teisių ir privatumo (JAV atvejis); 2. „švelnus“ neapsisprendimas dėl, viena vertus, inovacijų nevaržomos plėtros skatinimo ir, kita vertus, žmogaus teisių pažeidimų užkardymo (ES atvejis); 3. baimė, kad skaitmeninius duomenis gali rinkti nedraugiškai nusiteikusi valstybė, Kinija (Lietuvos atvejis).
Reikšminiai žodžiai: vizualioji kontrolė ir VA, sekimo kapitalizmas, biometrinių duomenų nuosavybė, privatumo sampratos, emocijų (ne)atpažinimas.

Visual Control in Today's Societies: (Non)Recognition of Faces and Emotions

Summary. By using a theoretical approach to the critique of surveillance capitalism, and by drawing on public discourse sources on facial recognition (FR) technology, this paper analyzes visual surveillance in contemporary societies. Currently, there are both numerous instances of a sudden development of FR capabilities on a global scale as well as efforts

Received: 02/12/2021. **Accepted:** 11/03/2022

to prevent the development of what is called the "most dangerous technology." This paper also questions the techno-solutionism that enables "perfect" mathematical human cognition. Overall, the paper sheds light on the global disagreement on the regulatory environment for FR technology, with different countries, states, or big cities treating biometric data protection differently. There is also a confluence of predicaments and legal concerns in the public sphere regarding FR. Nevertheless, it is possible to outline the typical narratives that emerge in media discourses, highlighted in this paper using three different examples. These are (1) concerns about human rights and privacy (the US case), (2) a "soft" indecisiveness about promoting unfettered innovation on the one hand, and preventing human rights abuses on the other (the EU case), and (3) the fear of digital data being collected by a hostile authoritarian state, namely China (the Lithuanian case).
Keywords: visual control and facial recognition, surveillance capitalism, ownership of biometric data, definitions of privacy, (non)recognition of emotions.

Įvadas

Viešojoje politikoje daug dėmesio sulaukia nauji skaitmeninės valdysenos, algoritmų kontrolės ir administravimo būdai. Ne tik keliami klausimai apie informacinių ir komunikacinių technologijų (IKT) galimybes ar efektyvesnius problemų sprendimus, bet ir išsakomas rūpestis dėl šališkų technologijų poveikio ir žmonių privatumo išsaugojimo. Šiandien jau ne paslaptis, kad vadinamųjų išsivysčiusių valstybių institucijos (ir ne tik policija ar saugumo agentūros) dideliu mastu renka ir naudoja biometrinius asmens atpažinimo duomenis – akies rainelių, pirštų atspaudų ar veidų atvaizdus. Pasaulinės pandemijos situacijoje privačios bendrovės valstybės agentūroms taip pat siūlo asmens sveikatos identifikavimo ir ligos požymių atpažinimo paslaugas, taigi viešose vietose vis dažniau pastebimi įvairūs asmens fizinę būklę fiksuojantys įrenginiai, kaip antai per atstumą žmogaus temperatūrą matuojantys ekranai, medicininių kaukių (ne)dėvėjimą matančios kameros ir pan.

Technologijų politiką aptariančioje literatūroje ir žiniasklaidoje dirbtinio intelekto (DI) ekspertai, nevyriausybinės organizacijos ir kai kurie politikai ne veltui pabrėžia, kad inovatyvius matavimo, sekimo ir stebėjimo įrenginius gaminančios bendrovės tampa nuolatinėmis viešosios politikos (sveikatos ir socialinių paslaugų sistemos) administratorėmis, lemiančiomis svarbius sprendimus, kurie kyla iš

visuomenei niekaip neprieinamos (o kartais ir netikslios) informacijos[1]. Kai skaitmeninių automatizuotai gaunamų duomenų nuosavybė nėra iki galo apibrėžta, o reglamentavimo terpė ir asmens apsaugos režimai dar tik formuojasi, tradicinė viešojo ir privataus sektorių skirtis neretai ne tik praranda aiškesnes ribas, bet ir prasmę. Taigi šiandien dažnai konstatuojamas IKT proveržis duomenų rinkimo ir sekimo programinės įrangos versluose[2]; apie technologijų teikiamas pozityvias galimybes nuolat kalbama inovacijas skatinančių vyriausybių agentūrų pranešimuose, technologijų žiniasklaidoje, kai kurių mokslininkų ir sumanių įrankių kūrėjų pasisakymuose. Tačiau lygia greta diskutuojama apie kai kurių duomenų bazių (ne)patikimumą, netikėtai išryškėjusį vienos ar kitos bendrovės kuriamų modelių šališkumą, algoritminę diskriminaciją. Aiškinamasi ir apie asmens privatumo sampratas bei tai, ką reiškia būti nuolat matomam (-ai), sekamam (-ai), atpažįstamam (-ai) ir klasifikuojamam (-ai) mašinų.

Aptariant vizualiosios populiacijų kontrolės klasifikacijos būdus technologijų požiūriu, galima išskirti pagrindines biometrines matavimo ir sekimo priemones. Jos gali būti skirstomos pagal duomenų tipus, kurie siejami su: 1. biologiniais duomenimis (kaip antai kūno įkalčiai kriminologijoje); 2. vizualiaisiais ar garsiniais duomenimis (veidas, balsas, piršto arba delno atspaudo vaizdas); 3. skaitmeniniais duomenimis (tam tikri žmogaus elgsenos pėdsakai elektroninėje erdvėje)[3]. Konkrečiai šio teksto atveju vizualiosios kontrolės analizei

---

1 Dave Gershgorn, „We Mapped How the Coronavirus is Driving New Surveillance Programs Around the World“, *onezero.medium* (2020 m. balandžio 9 d.), *https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9*.

2 Kalbos atpažinimas, vaizdų atpažinimas ir su tuo susiję įrankiai šiuo metu yra perspektyviausios dirbtinio intelekto (DI) sritys, įmonėms ir šalims duodančios įspūdingus kasmet didėjančius pelnus. Mat tokių įrankių algoritmų mokymui pradėtos naudoti milžiniškos duomenų talpyklos ir vis galingesni kompiuteriai.

3 Populiarioje žiniasklaidoje šias skirtis gana aiškiai pristatė su biometriniais duomenimis dirbantis Lietuvos matematikas informatikas ir DI tyrėjas Linas Petkevičius, žr. Linas Petkevičius, „Asmenį identifikuojančios technologijos kasdienybėje – daugiau saugumo ar mažiau privatumo?“, *15min.lt* (2020 m. gruodžio 7 d.), https://www.15min.lt/gyvenimas/naujiena/laisvalaikis/asmeni-identifikuojancios-technologijos-kasdienybeje-daugiau-saugumo-ar-maziau-privatumo-1038-1418332?copied.

pasirenkama politiškai bene prieštaringiausia veidų atpažinimo (VA) technologija. Ji taip pat turi įvairių tipų ir pogrupių[4]. Vis dėlto VA technikų arsenalas šiame tekste neaktualizuojamas – vienodai vertinama galimybė atpažinti veidą tiek iš saugumo kameroje fiksuoto vaizdo, tiek iš interneto erdvėje egzistuojančios fotografijos. Taip pat pritariama minčiai, jog klasifikacijose dažnai linksniuojama veido analitika (angl. „*face analysis*“) yra vienas kontroversiškiausių asmens „gilesnio“ pažinimo būdų. Mat veido analizės potencialas pagal įvairias žmogiškumo „skales“ dažnai klaidina, nes individualių charakteristikų ir išraiškų prasmė yra nepastovi ir socialiai konstruota, o ne determinuota matematiškai[5].

Taigi pabrėžiant ne techninę matymo būdų įvairovę, bet ideologinius ir kultūrinius VA aspektus, veido vaizdas šiuo atveju traktuojamas kaip savaime jautrus personifikacijos ženklas – ne tiek biometrinių duomenų talpykla, kiek su asmens orumu susijęs unikalios identifikacijos simbolis. Dar ne taip seniai VA technologijos taikymas viešojoje politikoje buvo „natūralus“ *tabu* dėl pernelyg radikalaus įsibrovimo į privatumo sritį. Vis dėlto šiandien visuomenės nuostatos kinta, nes darosi vis sunkiau pasislėpti kamerų ir panašių sekimo sensorių „prifarširuotame“ pasaulyje, tiek skaitmeninėje, tiek fizinėje erdvėje. Kad ir kaip žiūrėsime, šiuolaikinis individas jau nebėra nematomas išorinei (mašinos) akiai – jo(s) identifikacija kasdien tampa vis lengvesnė tiek autoritarinėse, tiek demokratinėse valstybėse. Tai, savo ruožtu, provokuoja pasipriešinimą beprecedenčiam sekimo režimui ir paskatina naujus veido atvaizdo nuosavybės ir asmens integralumo klausimus. Taigi ir šio teksto atveju sekimo ir duomenų rinkimo procesas siejamas su implikacijomis asmens identiteto sampratai ir privatumo dezintegracijos baime.

---

4 Apie VA ir skirtingo lygmens identifikavimo bei sekimo tipologijas plačiau žr. Adam Schwartz, „Resisting the Menace of Face Recognition“, *Electric Frontier Foundation* (2021 m. spalio 26 d.), https://www.eff.org/deeplinks/2021/10/resisting-menace-face-recognition.

5 Veido analitika siejasi su veido analizei skirtais sudėtingesniais algoritmais, siekiančiais atpažinti žmogaus emocines būsenas ir kitas savybes, t. y. tik pagal veido duomenis siekiama tiksliai identifikuoti rasinę ar etninę priklausomybę, netgi seksualinę orientaciją. Žr. Adam Schwartz, ten pat.

Pasitelkiant sekimo kapitalizmo, duomenų kolonializmo bei algoritminio valdymo[6] kritikos teorinę prieigą ir naudojantis viešojo politinio diskurso (žiniasklaidos) medžiaga, vizualioji kontrolė straipsnyje analizuojama iškeliant VA technologijos plėtrą lydinčias prieštaras. Iš dalies šias prieštaras galima apibūdinti kaip konfrontaciją tarp technologinio determinizmo (arba *techno solutionism* paradigmos)[7] ir kritinio požiūrio į (vis dar) nereguliuojamą VA technologijų arsenalą. Rūpinantis žmogaus teisių apsauga ir samprotaujant apie privatumo ribas skaitmeninio identiteto radikalaus neapibrėžtumo kontekste, tampa akivaizdu, kad kol kas nėra teisinio, filosofinio ar kultūrologinio konsensuso dėl to, kurioje vietoje turėtų „įsikišti“ įstatymus kurianti valstybė. Skirtingose šalyse, paskirose valstijose ar miestuose kuriami savi teisiniai režimai, o biometrinių duomenų apsauga traktuojama nevienodai. Taigi natūralia medžiaga dabarties „neapibrėžtumo situacijai“ apžvelgti tampa VA klausimus analizuojantys informaciniai užsienio technologijų žiniasklaidos pranešimai, technologijų žurnalistų ir akademikų – DI tyrėjų, teisininkų, filosofų ir pan. – perspėjimai, įžvalgos, taip pat valstybės institucijų, politikų ar nevyriausybinių organizacijų pareiškimai[8]. Daugiausia empirinių duomenų, politinių precedentų ir VA technologijos reklamos, taip pat kritikos galima aptikti JAV kontekste; ši šalis išsiskiria ir kalbant apie pilietinį bei politinį pasipriešinimą VA, be to, šios technologijos suspendavimą ar netgi visišką uždraudimą.

---

6 Pažymėtina, kad kalbant apie algoritmais besiremiantį administravimą dažnai vartojamas ir algoritminės valdysenos (kaip valdymo būdų visumos) terminas.

7 *Technosolutionism* – terminas, kurį JAV technologijų ir medijų tyrėjas Evgenyjus Morozovas sieja su „postinternetinės“ eros kompiuterių mokslo ir inovacijų politikos palaikomu siekiu išspręsti faktiškai visas šiuolaikiniam žmogui kylančias problemas pasitelkus būtent technologines priemones. Žr. Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York : Public Affairs, 2014).

8 Maždaug nuo 2017 m. pradėjus aktyviau kalbėti apie VA technologijas, būtent žiniasklaidos cituojami šaltiniai, labiau nei akademinė literatūra (kurios publikavimas yra kur kas lėtesnis procesas), leidžia matyti šioje srityje dirbančių ir viešojoje erdvėje pasisakančių akademikų refleksijas. Dėl ribotos teksto apimties minimi tik kai kurie tipiški informaciniai šaltiniai.

Kalbant apie emocines reakcijas, taip pat reikia pabrėžti, kad viešojoje erdvėje su VA technologija susiję precedentai bei politiniai ir teisiniai nuogąstavimai susipina. Vieni su konkrečiais atvejais susiję aspektai nereiškia, jog lygia greta neegzistuoja kiti. Tarkime, žiniasklaidoje aptariant sekimo ir didelio masto duomenų rinkimo automatizavimo procesus dažnai ne tik baiminamasi asmens privatumo pažeidimo, bet ir atkreipiamas dėmesys į geopolitines įtampas, komercinių paslapčių išviešinimo, kibernetinių išpuolių, t. y. įsilaužimo į valdymo sistemas, grėsmes. JAV biometrinių duomenų rinkimo (kartu ir VA) technologijos kritikuotos ne tik dėl neva „netyčinio" rasinio profiliavimo; čia plačiai kalbėta ir apie šalies saugumo požiūriu nepageidautinus „kiniškus algoritmus". Lietuvos žiniasklaidoje daugiausia minėtas tik pastarasis sekimo technologijų aspektas. Šio teksto trečiojoje dalyje kalbant apie didėjančias politines vizualiosios kontrolės prieštaras pasirinkti ne visi, o tik kai kurie tipiški nuogąstavimai. Tai – 1. rūpestis dėl žmogaus teisių ir privatumo (JAV atvejis); 2. „švelnus" neapsisprendimas dėl, viena vertus, IKT inovacijų plėtros kuo efektyvesnio skatinimo ir, kita vertus, žmogaus teisių pažeidimų užkardymo (ES atvejis); 3. baimė, kad skaitmeninius vizualiuosius duomenis gali nejuntamai rinkti nedraugiškai nusiteikusi valstybė – Kinija (Lietuvos atvejis).

1. Link maksimaliai objektyvaus asmenybės pažinimo?

Technikos filosofijoje kartais priešpriešinamos technologinio ir kultūrinio determinizmo nuostatos, kurios diskusijose apie naująsias medijas neretai tapatinamos su priešprieša tarp technologijų vertybinio neutralumo tezės ir jai oponuojančios technologijų intencionalumo tezės. Pastaroji nuostata tarsi suponuoja, kad žmogaus išrasti ir ištobulinti įrankiai (per)formuoja patį žmogų, kuriantį savo tikslams dar efektyviau tarnaujančius naujesnius (arba, kalbant šiuolaikiškiau, „sumanesnius") įrankius. Vis dėlto kai didžiųjų duomenų sankaupose ištobulėję vadinamieji mašininio mokymo algoritmai pradėjo dalyvauti viešojoje politikoje, žmogus kaip subjektas tarsi „pasitraukė į

šalį“. Kitaip tariant, lygia greta su technikos filosofijoje aptariama „dviašmenės“ inovacijų prigimties idėja (kai tas pats išradimas gali ir padėti, ir pakenkti) svarbu suprasti tai, kad automatizuoto algoritminio valdymo kontekste[9] individualios intencijos eliminuojamos. Mat duomenų rinkimas ir apdorojimas priimant sprendimus veikia sunaikinus skaitmeninius pėdsakus „paliekančio“ asmens subjektyvumą. Algoritminio valdymo ir valdysenos tezės sugestijuoja „grynojo“ kompiuterių ir duomenų mokslo įgalintą „skaitmeniniu žinojimu“ besiremiantį valdymo ir administravimo procesą.

Filosofinis technikos priemonių (neutralumo) klausimas gali būti siejamas ir su ideologinio neutralumo tezėmis. Pasak vokiečių technikos filosofo Günterio Ropohlo, ideologinio vertės neutralumo problematikos apžvalga nesunkiai pailiustruoja, kad ideologija iš principo gali būti pasitelkiama prieštaringoms pozicijoms pagrįsti[10]. Visuomenės automatizacijos ir algoritminės valdysenos procesus kritiškai analizavęs Bernardas Stiegleris išryškino technologinio ir biologinio automatizmo ir šių sistemų autonomijos problemas, akcentuodamas automatizuoto žinojimo dviprasmybę[11]. Panašiai, dviprasmiškame ir prieštaringame ideologiniame kontekste – vis efektyvesnio problemų sprendimo pasitelkiant technologijas, iš vienos pusės, ir grėsmių bei pavojaus asmens integralumui, iš kitos pusės, lauke – galime vertinti ir VA technologijos raidą. Kalbant apie ideologinę technikos neutralumo nuostatą šiuo atveju verta atkreipti dėmesį ir į pirmenybės teikimą

---

9 Apie algoritminį valdymą grindžiančias algoritminės valdysenos idėjas plačiau žr.: Antoinette Rouvroy ir Thomas Berns, „Algorithmic Governmentality and Prospects of Emancipation. Disparateness as a Precondition for Individuation through Relationships?“ (translated by Elizabeth Libbrecht), *Réseaux*, Volume 177, Issue 1 (2013): 163–196; Ignas Kalpokas, *Algorithmic Governance: Politics and Law in the Post-Human Era* (Cham: Palgrave Macmillan, 2019).

10 Tai, pasak teoretiko, iliustruoja pats techninės pažangos tezės prieštaringumas: „[i]nžinieriai ir technikos optimistai negali daugiau teisinti technizacijos proceso sakydami, kad jis nekelia tam tikrų pavojų, tačiau technikos pesimistai taip pat negali daugiau neigti, kad techninių problemų sprendimu visuomet siekiama lengvinti ir gerinti žmonių gyvenimo praktiką.“ Žr. skyrių G. Ropol, „Techninis problemų sprendimas“, in *Technikos filosofijos įvadas* (Vilnius: Kultūros ir meno institutas, 1998), 266.

11 Bernard Stiegler, „The Future of Work“ (translated by D. Ross). *Automatic Society* 1 (2016) (Cambridge, Malden: Polity Press).

pačiam matematiniam normatyvumui dėl tikslesnio bei geresnio žmogaus pažinimo. Alexanderis Campolo ir Kate'ė Crawford, pavyzdžiui, kalba apie „determinizmo burtus" (angl. *enchanted determinism*), kai mašininio mokymosi algoritmai produkuoja sudėtingas racionalų žinojimą transformuojančias, mus „apkerinčias" skaičiavimo ir prognozavimo sistemas, o technooptimistai ir algoritmų kūrėjai siūlo jomis besąlygiškai tikėti. Antžmogiškos gebos mašinos tarsi leidžia neprisiimti jokios atsakomybės už procesus, ratifikuojančius socialinę kontrolę ir žmogui jau natūraliai nebesuprantamas klasifikacijas[12].

Konkrečiai šio teksto atveju pabrėžiama būtent tokio žinojimo ambivalencija – pavyzdžiui, socialiniai mokslai dažnai tyrinėja jau nebe žmogaus ir technologijų santykį, bet algoritminio valdymo erdvėje funkcionuojančio ir reguliuojamo „žinojimo apie žmogų" santykį su automatinėmis sistemomis[13]. Tai, kaip šis duomenimis grįsto reguliavimo režimas sutrikdo žmogaus integralumą bei privatumą, istoriniu požiūriu plačiai analizavo ir socialinė psichologė Shoshana Zuboff, suformulavusi sekimo kapitalizmo (angl. *surveillance capitalism*) tezes[14]. Pasak jos, didžiųjų duomenų akumuliavimo procese bet kuri gyvoji patirtis gali būti paverčiama „elgesio duomenimis" ir monetizuojama, o eiliniams vartotojams nematomi ir niekaip nepažinūs patirties grobimo procesai apima visas šiandien įmanomas biometrinių duomenų rinkimo technologijas[15].

---

[12] Alexander Campolo ir Kate Crawford, „Enchanted Determinism: Power without Responsibility in Artificial Intelligence", *Engaging Science, Technology, and Society* Vol. 6 (2020), DOI: https://doi.org/10.17351/ests2020.277.

[13] Eric Bogert, Aaron Schecter ir Richard T. Watson, „Humans rely More on Algorithms Than Social Influence as a Task becomes More Difficult", *Scientific Reports* (2021), https://www.nature.com/articles/s41598-021-87480-9.

[14] Autorė išsamiai analizavo globalią skaitmeninę architektūrą, kuri kolonizuoja privačią patirtį ir modifikuoja žmogaus prigimtį, panašiai kaip industrinis kapitalizmas modifikavo gamtinę aplinką XIX–XX a. Zuboff suformuluotas pagrindines sekimo kapitalizmo įžvalgas plačiau esu pristačiusi kitur: žr. Skaidra Trilupaitytė, „Spąstai žmogaus pasauliui", *Athena: filosofijos studijos*, nr. 16 (2021).

[15] Zuboff plačiai aprašo istorinę atpažinimo ir biometrinio sekimo įrankių plėtrą, kurią ji įvardija kaip vis labiau užgrobiamas kūno skaitmeninės identifikacijos sritis, apimančias žmonių organus, kraują, akis, smegenų bangas, veidus, eiseną, laikyseną. Žr.: Shoshana Zuboff, „The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power", *Public Affairs* (2019): 262–263.

Zuboff nuosekliai kritikavo ir duomenų mokslo kontekste susidariusią nuostatą, kad „galutinė tiesa“ apie žmogų galiausiai randasi statistiškai apskaičiuojamoje realybėje. Pavyzdžiui, mokslininkė itin skeptiškai vertino tam tikras KIT įmonių plėtojamas inovacijų strategijas, kurias ji siejo ir su biheiviorizmo psichologija bei radikalių šios srities XX a. vidurio atstovų, tokių kaip B. F. Skinneris, darbais (panašias idėjas vertinant žmonių populiacijas vėliau pratęsė ir plėtojo kompiuterių mokslas, pavyzdžiui, Zuboff plačiai kvestionuoja šio mokslo atstovo Alexo Pentlando įžvalgas). Žmogiško subjekto intencionalumo eliminavimą automatizuotos viešosios politikos kontekste kritiškai vertino ir kiti internetinių medijų teoretikai[16]. Didžiųjų duomenų grobimą lyginant su kolonijinėmis kapitalistinės ekonomikos grobimo ir naudojimo praktikomis (kaip antai žemių ar kitokių išteklių kaupimas), teorinė dekolonizacijos perspektyva šiuo atveju taip pat gali būti pravarti priešinantis matematinio instrumentalizmo diskursui, jam priešpriešinant asmens skaitmeninio integralumo ir duomenų nuosavybės klausimus[17].

Matymo technologijas analizavęs teisės ir technologijų teoretikas Jake’as Goldenfeinas, remdamasis naujais VA pavyzdžiais, panašiai kaip ir kiti, kvestionavo kompiuterių mokslų ir ypač mašininio mokymo(si) lauke besiformuojančią prielaidą, kad individų ir populiacijų pažinimas yra neva neutralus ir maksimaliai „objektyvus“. Tyrėjas parodė, kokiais būdais kiekviena naujai atrasta vizualioji technologija suteikė žmonėms galbūt patikimesnę (objektyvesnę) prieigą prie ligi tol mūsų akiai nepastebimų dalykų[18]. Savo ruožtu, kai kurių

---

16 JAV medijų teoretikas ir viešasis intelektualas Douglas Rushkoffas, ne sykį kvestionavęs Silicio slėnio atstovų strategijas ir retoriką, taip pat siūlė grąžinti algoritminio valdymo sprendimams žmogiškumo dimensiją. Žr. Douglas Rushkoff, *Team Human* (New York: W. W. Norton & Company, 2019), 173–183.

17 Nick Couldry ir Ulises Mejias, „The Decolonial Turn in Data and Technology Research: What is at stake and where is It Heading?“, *Information, Communication & Society* (2021, Nov 9 d.), https://doi.org/10.1080/1369118X.2021.1986102.

18 Pavyzdžiui, XIX a. užgimusi fotografija netrukus buvo pradėta traktuoti kaip būdas „pažvelgti giliau“; panašiai buvo manoma ir apie vėlesnes matymo technologijas. Žr. Jake Goldenfein, „Facial Recognition is Only the Beginning“, *Public Books* (2020, 26 Mar), https://ssrn.com/abstract=3546525.

šiandien įtakingų tiksliųjų mokslų tyrėjų darbai neblogai iliustruoja, kokiu būdu technologijų pažanga natūraliai tapatinama su moksliniu objektyvumu (ypač kai matematiniais modeliais grįstos žinios skverbiasi į kompiuterinio matymo bei veidų „apskaičiavimo“ sritį). Tarkime, svarbaus VA tyrimų srities atstovo Michalo Kosinskio tekstuose parodoma, kad su DI algoritmų nepažinumu ir juodąja dėže siejama VA technologija analizuoja veidus pagal išorinius nekintančius (forma) ir kintančius (išraiška, makiažo ar šukuosenos stilius, galvos padėtis) bruožus, pagal visus veido duomenis tiksliai nustatydama amžių, lytį, seksualinę orientaciją ar etninius požymius. O svarbiausia – technologija tai daro geriau nei žmogus[19]. Šią epistemologinę poziciją, kurios laikomasi vertinant žmones, Goldenfeinas įvardijo kaip komputacinį empiricizmą (angl. *computational empiricism*). Tai yra tam tikra žinojimo prielaida, kai žmogų identifikuojančia ir apibūdinančia mašina pradedama pasitikėti labiau nei tuo, kaip patys žmonės identifikuoja save.

Viešosios politikos lygmeniu šią technologijų vertybinio neutralumo nuostatą iliustruoja pirmenybės teikimas „sumanesniam už žmones“ įrenginiuose esančiam DI. Juk ir darbo aplinkoje ar asmeniniame gyvenime žmonės neretai skatinami netiesiogiai pasinaudoti matematinėmis veido analitikos galimybėmis (į telefoną įdiegtomis ir potencialių partnerių veido bruožus „teisingai interpretuojančiomis“ susipažinimo programėlėmis, priimant naujus darbuotojus į darbą žmones analizuojančiomis vaizdo programomis ir pan.[20]). Savo ruožtu, siekiant efektyvesnio automatizuoto viešosios erdvės administravimo, ne vienoje šalyje (ne tik Kinijoje) automatiškai mėginama atpažinti ryškiausias emocines praeivių mieste būsenas tam, kad policija laiku identifikuotų agresyviai nusiteikusius ir galbūt

[19] Yilun Wang ir Michal Kosinski, „Deep Neural Networks are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images“, *Journal of Personality and Social Psychology* 114, nr. 2 (2018).

[20] Victor Tangermann, „Could This Neural Network Really be better at predicting Personality Traits Than Humans?“, *Futurism* (2020 m. gegužės 22 d.), https://futurism.com/researchers-ai-judge-personality-selfies.

nusikaltimus linkusius daryti asmenis. Praeivių emocijas identifikuojančios VA sistemos, skirtos (būsimų) nusikaltimų užkardymui, populiarėja ne vienoje šalyje[21]. Technologija plinta nepaisant to, kad galimų kriminalinių nusikaltėlių išankstinį automatizuotą „išaiškinimą“ kartais lydi nesusipratimai ir kuriozai[22]. Lygia greta predikcinė kontroliavimo politika sulaukia pelnytos kritikos[23]. Juk algoritminės valdysenos erdvėje susiformavę anoniminiai matematinio administravimo modeliai galiausiai transformuojami į labai konkrečios politinės ar ekonominės galios valioje esančius įrankius. Vizualioji kontrolė technologiškai išsivysčiusiose valstybėse iš matematinio matymo bei žinojimo erdvės eliminuoja bet kokį subjektyvumą. Būtent todėl instrumentinės anoniminio *Didžiojo Kito* (pasak Zuboff) intencijos optimizuoti emocijas ir elgesį iš tiesų sugestijuoja gana distopinį scenarijų, o tai platesniame VA politikos kontekste verčia abejoti ideologine technikos neutralumo nuostata. Vykstant technologijų proveržiui, aštrėja ir jas supančios prieštaros.

2. Tarp staigios VA plėtros ir „pačios pavojingiausios technologijos“ užkardymo

Privatumo sampratų (ir atitinkamai – teisinio reguliavimo nuostatų) kaita paprastai neatsiejama nuo technologinių inovacijų plėtros kultūrinių aplinkybių, tai rodo ir vaizdų (at)pažinimo technikų istorinis

---

21 Plačiau žr.: Dave Gershgorn, „Aggression Detection' is Coming to Facial Recognition Cameras Around the World“, *onezero.medium* (2020 m. rugsėjo 25 d.), https://onezero.medium.com/aggression-detection-is-coming-to-facial-recognition-cameras-around-the-world-90f73ff65c7f; Cho Mu-Hyun, „Seoul to install AI Cameras for Crime Detection“, *ZDNet* (2020 m. sausio 2 d.), https://www.zdnet.com/article/seoul-to-install-ai-cameras-for-crime-detection/.

22 Hugh Bronstein, „Rights Group criticizes Buenos Aires for Using Face Recognition Tech on Kids“, *Reuters* (2020 m. spalio 9 d.), https://www.reuters.com/article/uk-argentina-rights-idUKKBN26U208.

23 Heaven W. Douglas, „Predictive policing Algorithms are Racist. They Need to be dismantled“, *MIT Technology Review* (2020 m. liepos 17 d.), https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

kontekstas. Tarkime, kompiuterinio matymo (angl. *computer vision*) rudimentų buvo žinoma jau maždaug nuo XX a. septintojo dešimtmečio, bet tik pastaraisiais metais sparčiai tobulėjančios technologijos įgalino VA ir asmenų identifikavimą itin plačiu mastu ir realiu laiku. Taigi, nors policijos departamentai įvairiose pasaulio šalyse jau ne pirmą dešimtmetį naudoja paprastesnes VA įrankių variacijas, iki šiol viešojoje erdvėje nekilo pernelyg aštrių problemų dėl piktnaudžiavimo jais. Mat asmens atpažinimo galimybes tam tikra prasme ribojo vaizdų duomenų bazės (nusikaltėlių nuotraukos arba paso ar vairuotojo pažymėjimo fotoatvaizdai), kurios yra vyriausybių nuosavybė.

Dėl minėtojo su DI susijusių inovacijų proveržio pastaraisiais metais situacija smarkiai kito, o kompiuterio gebėjimas automatiškai atpažinti žmogų iš veido atvaizdo tobulėjo. Netgi kai kurios anksčiau tuo nesidomėjusios didžiosios JAV technologijų įmonės (*Big Tech*), kaip antai „Amazon“, ėmė pardavinėti valstybinėms saugumo agentūroms VA technologijos produktus, veikiančius bet kurios duomenų bazės pagrindu. Lygia greta technologijų žiniasklaidoje (visų pirma JAV) imta teigti, jog naujieji matematiniai modeliai, deja, neišvengia klaidų, o automatizuotai veikiantys algoritmai gali tapti šališki ir diskriminuojantys. Inovatyvių produktų kūrėjai susidūrė su rimtais sunkumais, kai buvo pradėti plačiai aptarinėti „neapsižiūrėjimo“ atvejai, pavyzdžiui, „Google“ bendrovės fotografijų VA algoritmas 2015 m. pažymėjo porą atsitiktinių juodaodžių asmenų kaip „gorilas“. Vis dažniau minėta ir tai, kad autoritarinėse šalyse VA inovacijos ne tik tarnauja viešojo sektoriaus administravimui, bet ir veikia kaip nuolatinės visa apimančios priežiūros bei represijų įrankis (itin dažnai minimas pavyzdys – Kinijos vakaruose esančią Sindziango vietovę apraizgę kamerų tinklai – idealios policinės valstybės pavyzdys).

Daugiausia nerimo ėmė kelti būtent algoritmų „įdarbinimas“ viešojoje politikoje – sekimo, atpažinimo ir profiliavimo sistemos nemaža apimtimi veikia ir sprendimus siūlo (beje, kartais klaidingus ir diskriminuojančius) JAV darbo rinkoje, nustatant bausmės laikotarpį įkalinimo įstaigose, teikiant paskolas, socialines paslaugas, teismo

procesų metu ir kitose gyvenimo srityse[24]. Taigi kartu pradėta mąstyti apie griežtesnę kontrolę ir visų pirma pačių įrankių reguliavimą. Jau 2016 m. JAV nacionalinė telekomunikacijų ir informacijos administracija paskelbė VA naudojimo gaires, kuriose prašoma, kad įmonės technologiją taikytų skaidriai, o duomenys būtų valdomi „tinkamai“; čia taip pat rekomenduojama, kad vartotojai turėtų galimybę kontroliuoti dalijimąsi jų veido skaitmeniniais duomenimis su trečiosiomis šalimis[25]. Vis dėlto išoriniams stebėtojams vėliau liko neaišku ar (ir kaip) VA technologijos gamintojai laikėsi gairėse nurodytų pageidavimų.

Nepaisant tarptautinėje žiniasklaidoje fragmentiškai minėtų nemalonių precedentų ir perspėjimų, efektyvėjant technologijai toliau plito ir VA „įdarbinimas“. Kameros „nuskaitomu“ veidu atsirakinami išmanieji telefonai (nuo 2017 m.), galima užsisakyti maistą ir susimokėti greitojo maisto restorane ar parduotuvėje. Ne sykį reklamuota VA priemonėmis įgalinta prieiga prie asmeninių namų saugumo sistemų, bankininkystės paslaugų, kalbėta apie naujos kartos kameras prekybos centruose, veidų sekimą išmaniuosiuose reklamos stenduose. Atpažinimas naudojant kameras vis dažniau pasitelktas oro uostų saugumui užtikrinti (taip pat akimirksniu identifikuojant keleivius), darbuotojų patekimui į biurą, įvairiuose policijos stebėjimo procesuose, išmaniuosiuose akiniuose, prie saugos darbuotojų aprangos tvirtinamose „kūno kamerose“ ir t. t. Taigi VA technologija ne veltui traktuota ir kaip ateityje tiesiog neišvengiama mūsų kasdieniame gyvenime, pačiose įvairiausiose situacijose; iš esmės visame pasauly-

---

24 Viena pirmųjų predikcinių algoritmų pavojus plačiau aprašė JAV matematikė ir duomenų mokslininkė Cathy O'Neil. 2016 m. pasirodžiusi jos knyga *Matematinio naikinimo ginklai* pateikė daugybę nematomos diskriminacijos pavyzdžių viešajame sektoriuje. Žr. Cathy O'Neil, *Weapons of Math Destruction* (New York: Crown Books, 2016). JAV algoritminės diskriminacijos atvejus taip pat išsamiai aptaria prie Niujorko universiteto įkurto *AI Now* instituto metinės ataskaitos ir kitų nevyriausybinių organizacijų tyrimai.

25 Privacy Multistakeholder Process: Facial Recognition Technology, *United States Department of Commerce* (2016 m. birželio 17 d.), National Telecommunications and Information Administration, https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology.

je[26] (kompiuterinio matymo sistema taikyta mažmeninėje prekyboje ir Vilniaus senamiestyje, kur trumpai veikė, kaip teigta, pirmoji Europoje „sumani“ parduotuvė be pardavėjų[27]).

Vis dėlto JAV pilietinės visuomenės grupių pranešimuose lygia greta gausėjo perspėjimų apie nemalonius precedentus ir grėsmes[28]. Daug sykių linksniuotas, pavyzdžiui, Amerikos pilietinių teisių sąjungos 2018 m. liepos pareiškimas, kad bendrovės „Amazon“ VA produktas – programinė įranga „Rekognition“ – po eksperimento klaidingai sutapatino 28 JAV Kongreso narius su policijos suimtų nusikaltėlių vaizdų talpyklos fotografijomis. Technologijų naujienas aptariančioje žiniasklaidoje vėliau skelbta, jog kai kurių JAV miestų policijos departamentai, taip pat Federalinių tyrimų biuras savo darbe irgi naudoja minėtąją „Rekognition“ programą; žiniasklaida išsiaiškino ir tai, kad „Amazon“slapčia mėgino įsiūlyti šį šališkumu pasižymintį įrankį JAV imigracijos institucijoms ir kitoms su teisinėmis procedūromis susijusioms ir kai kurias grupes galbūt diskriminuojančioms JAV agentūroms[29].

Dėl minėtų priežasčių maždaug nuo 2018 m. galima matyti visuomenėje didėjantį pasipriešinimą vis gilesniam technologijos įsismelkimui į viešojo administravimo sritį, prabilta apie realią grėsmę asmeninei žmonių erdvei. Tais metais netgi pasigirdo nuogąstavimų dėl to, kad VA yra pavojingiausia iš visų žmogaus išrastų sekimo ir kontrolės

---

26 Tom Simonite, „Facial Recognition is Suddenly Everywhere. Should You Worry?“, *WIRED.com* (2019 m. birželio 8 d.), https://www.wired.com/story/facial-recognition-everywhere-should-you-worry/.

27 „Dirbtinio intelekto valdomą parduotuvę sukūrusiam lietuvių startuoliui – milijono eurų investicija“, *15min.lt* (2020 m. rugpjūčio 5 d.), https://www.15min.lt/verslas/naujiena/bendroves/dirbtinio-intelekto-valdoma-parduotuve-sukurusiam-lietuviu-startuoliui-milijono-euru-investicija-663-1357492?copied&copied.

28 Madhumita Murgia, „Who's Using Your Face? The Ugly Truth about Facial Recognition“, *Financial Times* (2019 m. balandžio 19 d.), https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e.

29 Davey Alba ir Lissandra Villa, „As Concerns Over Facial Recognition Grow, Members of Congress are Considering Their Next Move“, *buzzfeednews.com* (2019 m. vasario 20 d.), https://www.buzzfeednews.com/article/daveyalba/house-oversight-committee-hearing-facial-recognition.

technologijų[30]. Retoriškai klausta, ar VA ilgainiui iš tiesų padės kurti saugesnę visuomenę, ar tiesiog greičiau nuves mus link autoritarinio distopinio panoptikono, kartu su kitomis į sumanias sistemas integruotomis sekimo priemonėmis sunaikinsiančio visas žmonių privatumo erdves (kas jau praktiškai egzistuoja Kinijoje)?[31] 2018 m. kompiuterių mokslų srityje pasirodė ir žiniasklaidoje vėliau linksniuotų tyrimų, teigiančių, kad VA technologijos gali akivaizdžiai tapti diskriminacijos, tradicinio rasizmo ir priespaudos įrankiu[32]. Iš svarbių VA kritikos šaltinių technologijų pasaulyje galima minėti 2018 m. paskelbtą ir vėliau dažnai žiniasklaidoje cituotą Masačusetso technologijų instituto mokslininkių Joy Buolamwini ir Timnit Gebru tyrimą[33].

Iš tiesų reikia pabrėžti, kad duomenų mokslo įgalintas ir „skaitmeniniu žinojimu“ besiremiantis valdymo ir administravimo procesas JAV dažnai demaskuojamas būtent su matematika susijusių ar gimininguų sričių mokslininkų. Savotiškai pavojų skelbiantį toną JAV, kalbant apie VA, daugiausia inspiravo, kaip minėta, ir patys IKT bendrovių atstovai bei nepriklausomi tyrėjai, kaip antai matematikė O'Neil. Komputerinių mašinų asociacijos (angl. *Association of Computing Machinery*) žurnale paskelbtas „Microsoft“ bendrovės tyrėjo Luke'o Starko VA technologijos palyginimas su itin pavojinga medžiaga – chemiškai radioaktyviu metalu plutoniu – buvo panaudotas netgi sąmoningai siekiant sukrėsti skaitytojus[34]. Plutonis yra

---

30 Woodrow Hartzog, „Facial Recognition is the Perfect Tool for Oppression“, *medium.com* (2018 m. rugpjūčio 2 d.), https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

31 Jon Christian, „How Facial Recognition could tear us Apart“, *onezeromedium.com* (2018 m. rugsėjo 17 d.).

32 Hartzog, 2018.

33 Šiuo atveju išryškinta, kad algoritmų treniravimo sistemoje glūdi šališki duomenys – paaiškėjo, jog kompiuteris vis „suklupdavo“ identifikuodamas tamsesnės odos spalvos moterų veidus. Žr.: Joy Buolamwini ir Timnit Gebru, „Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification“, in *Proceedings of Machine Learning Research*“ (PMLR'18) (New York: PMLR, 2018), 1–15.

34 Luke Stark, „Facial Recognition is the Plutonium of AI“, *XRDS* 25, nr. 3 (2019 spring), DOI: 10.1145/3313129, https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bf02eef1a16e422015f8/1555087116086/Facial+Recognition+is+Plutonium+-+Stark.pdf.

atominių elektrinių atlieka, energijos išgavimo procese gaunama šalutinė pavojinga metalo substancija, naudojama atominio ginklo gamyboje (medžiagos naudojimas šiandien yra itin stipriai ribojamas tarptautiniais susitarimais). Pasak vis platesnį VA naudojimą viešojoje politikoje kritikavusio L. Starko, nors ši pavojinga technologija pati savaime ir nekuria rasistinių prietarų, klasifikacinės VA sistemos turi pernelyg didelį potencialą pažadinti rasizmą kadaise maitinusius politinius instinktus – istoriniai duomenų bazių ir „žmogaus apskaičiavimo" metodų tyrimai tokias tendencijas tik paliudija[35]; panašias išvadas apie VA technologiją pateikė ir vizualiųjų klasifikavimo metodikų istoriniai tyrimai[36].

2019 m. kai kurie JAV miestai pradėjo skelbti apie pavojingos VA technologijos ribojimą arba visišką draudimą, tačiau turint mintyje itin plačią VA panaudojimo skalę ir didėjančias galimybes akimirksniu identifikuoti asmenį, nenuostabu, kad nuomonės apie pažeidimų ribas ir automatinio žmonių sekimo tikslus taip pat įvairuoja. Staigus apsipirkimas susimokant „tik veidu" neatrodo taip kontroversiškai kaip, tarkime, slaptas tos pačios VA įrangos naudojimas ugdymo įstaigose arba identifikuojant ir persekiojant konkrečius žmones (taip netiesiogiai slopinant gatvėse protestuojančių piliečių nepasitenkinimą). Arba „sumanios" parduotuvės mėginimas net neįspėjus lankytojų numatyti, kas iš jų gali būti potencialūs(!) vagišiai[37]. T. y. vieni žmonių atpažinimo ar sekimo tikslai ir būdai sulaukia kur kas mažiau visuomenės simpatijų nei kiti, o požiūriai į privatumą gali priklausyti ir nuo politinių institucijų ar netgi kultūrinių skirtumų. Demokratinėmis tradicijomis pastaraisiais dešimtmečiais nepasižyminčiose šalyse piliečių dalyvavimas automatizuoto atpažinimo procese gali

---

35 Stark, 2019, 53. Analogija su plutoniu turėjo aiškiai pailiustruoti VA įrankių pavojingumo mastą ir didelius naujų technologijų panašumus į aštrias XX a. vidurio pramonės sukeltas problemas (šios paskatino visuomenės sąmonėjimą ir naujų aplinkosaugos įstatymų atsiradimą).

36 Crawford ir Paglen, 2019.

37 Matt Burges, „Some UK Stores are using Facial Recognition to track Shoppers", *www.wired.com*. (2020 m. gruodžio 20 d.).

tapti privalomas norint funkcionuoti visuomenės gyvenime[38]. Tačiau JAV (ir ne tik) skirtingų miestų, valstijų ir centrinės valdžios politikai pradėjo aktyviau rūpintis žmogaus teisėmis ir priešintis privatumo pažeidimams; juk pastaruosius nuolat fiksavo bei viešino nepriklausoma žiniasklaida ir pilietinės visuomenės institutai.

Deja, staigios efektyvesnį visuomenės reguliavimą įgalinančių technologijų plėtros objektyviai pamatuoti ir išsamiai analizuoti šiuo metu beveik neįmanoma (nebent duomenys skelbiami viešai). Taip pat tikslesnė šalutinių neigiamų pasekmių prognozė negalima dėl komercinių paslapčių ir patikimų informacinių kanalų stokos (ne tik autoritarinėse šalyse). Fragmentiški skandalingi žiniasklaidos pranešimai liudija, kad tokios šalys kaip Kinija, pasitelkdamos VA, ne tik profiliuoja, bet ir masiškai persekioja bei represuoja piliečius, tam neretai naudojami kai kurių vakarietiškų *Big Tech* produktai. Kritikos sulaukė ir tai, kad, sprendžiant COVID-19 pandemijos sukeltas judėjimo kontrolės problemas, VA technologija buvo pasitelkiama demokratinių šalių mokyklose (viešai pernelyg to nė neskelbiant)[39]. JAV vykstant *Black Lives Matter* (BLM) protestams ryškėjo suvokimas, kad VA priemonės tarsi „netyčia“ tampa savotišku valdžios ir policijos ginklu, tai ypač iškalbingai iliustravo kai kurie skaudūs neteisingo juodaodžių suėmimo JAV miestuose precedentai. Žiniasklaidai atskleidžiant nemalonius faktus, taip pat smuko kai kurių specifinius sekimo įrankius gaminančių bendrovių reputacija, o tai, savo ruožtu, turėjo tolesnes politines implikacijas JAV kuriant naujus įstatymų projektus.

Kaip minėta, praktiniu lygmeniu apie universalesnes tarptautines kryptis kalbėti vargu ar yra prasmės, nes viešojo ir privataus sektorių institucijos skirtingose šalyse taiko netapačius VA ir žmonių stebėji-

---

38 „400 Million Indians Might soon Need to use Facial Recognition to access Their Bank Accounts“, *onezeromedium.com*., https://onezero.medium.com/access-to-welfare-programs-in-india-could-soon-depend-on-facial-recognition-scans-a09d21a96b1d.

39 Plačiau apie tai žr. „Schools adopt Face Recognition in the Name of Fighting Covid“, *www.wired.com.* (2020 m. lapkričio 3 d.). Žiniasklaidoje taip pat ne sykį skelbta, kad globali DI industrija pandemijos metu suintensyvino IKT ir priežiūros sistemų diegimą didžiausiose „nevakarietiško“ pasaulio šalyse.

mo standartus, o skirtingos šalys ir netgi miestai diegia savas taisykles. Juk, pasak technologijų inovatorių šūkių, technologijos tobulėja kur kas greičiau, nei jas reglamentuojanti „atsilikusi“ teisė. 2020 m. pradžioje žiniasklaida skelbė, kad kai kurių didžiųjų pasaulio miestų policija pradėjo plačiu mastu diegti VA sistemą realiu laiku (minėtas Londonas[40], Buenos Airės[41]). Reklaminėse didžiųjų miestų kampanijose taip pat galima matyti plintantį VA technologijos taikymą transporto sistemoje[42]. Skaitmeniniams įrankiams nejučia skverbiantis į kasdienį gyvenimą, šalių ir miestų vadovai kol kas neturi aiškaus galutinio atsakymo, koks pasitikėjimo lygis turėtų būti taikomas pusiau autonomiškoms sistemoms ir atpažinimo algoritmams. Dėl kokių priežasčių skirtingų šalių piliečiai sutiktų pažeisti kitų žmonių privatumo ribas ir koks būtų daugumą tenkinantis pa(si)teisinimas dėl populiacijų sekimo? Šie svarstymai veda link tolesnių prieštarų populiarinant ar kritiškai vertinant VA technologiją, kai ir propagavimas, ir kvestionavimas ar net arši kritika priklauso ne nuo tarptautinių įstatymų, o nuo konkrečios politinės situacijos ir kultūrinių bei akademinių tradicijų. Pastarosios leidžia kalbėti apie „griežtą“ kai kurių JAV valstijų ar miestų poziciją, „švelnesnę“ ES bendrosios politikos perspektyvą arba tokių ES valstybių kaip Lietuva žiniasklaidoje daugiausia pastebimą rūpestį dėl šalyje naudojamų skvarbių „Kinijos akių“.

---

40 Adam Smith, „The Met Police's Decision to use Facial Recognition not Only harms Our Right to Privacy – It damages Our Democracy, Too“, *Prospect* (2020 m. vasario 3 d.), https://www.prospectmagazine.co.uk/science-and-technology/met-police-facial-recognition-london-kings-cross-bias-uk.

41 Dave Gershgorn, „The U.S. Fears Live Facial Recognition. In Buenos Aires, it's a Fact of Life“, *onezero.medium* (2020 m. kovo 4 d.), https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.

42 VA sistema 2021 m. spalį įdiegta 240 Maskvos metro stočių; teigiama, jog tai pats plačiausias tokios sistemos panaudojimas pasaulyje, vis dėlto stebėtojams iš šalies susirūpinimą kėlė žmogaus teisių ir privatumo apsaugos klausimai: Ian Campbell, „Moscow adds Facial Recognition Payment System to More Than 240 Metro Stations“, *The Verge* (2021 m. spalio 15 d.), www.theverge.com/2021/10/15/22728667/russia-face-pay-system-moscow-metro-privacy.

3. Link tolesnės politinės prieštaros?

3.1. JAV valstijos ir miestai: skirtingi pasirinkimai

Būtent JAV kontekste patogiausia tirti ir tam tikras politines su VA susijusias prieštaras: šios šalies pilietinės ir akademinės organizacijos plačiai diskutuoja apie tai, kad statistiniai matematiniai metodai, taikomi, pavyzdžiui, klasifikuojant demografines gyventojų grupes, yra naudingi biopolitikos vadybai, o kartu nejučiomis tampa potencialiu (tradicinio) rasizmo įtvirtinimo įrankiu. Apie vizualiosios kontrolės priemonių pavojų JAV ėmė pasisakyti ne vien technologijų inžinieriai, bet ir kai kurie *Big Tech* vadovai[43]. Šios šalies pavyzdžiai – minėtasis „Rekognition“ įrankis ir kt. – plačiausiai aptarti žiniasklaidoje diskutuojant apie VA sistemų (kažkodėl) neatpažįstamą tamsesnę odos spalvą arba socialinį juodaodžių diskriminavimą. Taigi ir VA technologijos ribojimo ar net visiško draudimo tendenciją neatsitiktinai pradėjo JAV (minėtini kai kurie didieji Kalifornijos ir Masačūsetso valstijų miestai, pavyzdžiui, dažnai linksniuojamas San Franciskas). 2019 m. vasarį ir JAV centrinės valdžios institucijos pradėjo kvestionuoti veidų atpažinimo programos naudojimą šalies mastu, visų pirma didėjant susirūpinimui dėl potencialaus privatumo ir piliečių teisių pažeidimų[44]. Kita vertus, 2019 m. politinėse ir teisinėse diskusijose dar nebuvo iki galo aišku, pagal kokį JAV konstitucijos straipsnį vertinti VA technologijos plėtrą, poveikį žmonėms ir potencialius pažeidimus[45].

---

43 2018 m. liepą Bradas Smithas, „Microsoft“ prezidentas ir vyriausiasis patarėjas, ragino vyriausybę griežtai reguliuoti VA sistemas ir didinti įmonių socialinę atsakomybę už jas. Žr. Brad Smith, „Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility“, *Microsoft On the Issues* (2018 m. liepos 13 d.), https:// blogs.microsoft.com/on-the-issues/2018/07/13/ facial-recognition-technology-the-need-forpublic-regulation-and-corporate-responsibility/.

44 Davey Alba ir Villa Lissandra, „As Concerns Over Facial Recognition Grow, Members of Congress are Considering Their Next Move“, *buzzfeednews.com* (2019 m. vasario 20 d.), https://www.buzzfeednews.com/article/daveyalba/house-oversight-committee-hearing-facial-recognition.

45 „As Face-recognition Technology spreads, so do Ideas for Subverting It“, *economist.com (*2019 m. rugpjūčio 15 d.), https://www.economist.com/science-and-technology/2019/08/15/as-face-recognition-technology-spreads-so-do-ideas-for-subverting-it.

Kitaip tariant, nesant visuotinio aiškumo, kaip reglamentuoti VA praktikas, technologija lygia greta ir toliau sparčiai diegiama federalinės ir vietinės valdžios institucijose, oro uostuose, mažmeninėje prekyboje, mokyklose ir pan., o žiniasklaida pateikia „netikėtus“ ar šokiruojančius faktus. Visuomenėje ir tarp kai kurių politikų biometrinių duomenų siurbimo ir plėšimo kritika pasigirdo, kai didėjančias VA priemonių politines prieštaras paskatino sekimo poreikį 2020 m. suaktyvinusi pandemija ir tais pat metais JAV miestuose įsisiūbavę neramumai – protestai prieš juodaodžių diskriminaciją (BLM banga) – netiesiogiai suintensyvinę įvairaus pobūdžio kamerų naudojimą policijoje. Tuo metu pilietinės visuomenės diskusijose siekta įrodyti, kad nebus įmanoma sustabdyti JAV policijos smurto prieš juodaodžius piliečius, jei nebus užkardytas sofistikuotų stebėjimo priemonių naudojimas; teigta, jog visų pirma privalu uždrausti VA technologiją ir nutraukti subsidijas policijai šios technologijos įsigijimui. Buvo plačiau aptariami tokie precedentai kaip Detroite 2020 m. VA sistemos neteisingai identifikuoti bent du juodaodžiai praeiviai, kurie buvo neteisėtai suimti[46] (JAV buvo ir daugiau panašių atvejų). Detroito teisinės iniciatyvos ribojant VA netgi tapo savotišku modeliu kitiems miestams kuriant savus reglamentus[47].

JAV miestų pavyzdys rodo, kad lengviau vertinti skirtingus vietinės valdžios sprendimus, o ne šalies įstatymus, kurie dar tik kuriami. Mat bent jau šiuo metu reglamentavimo skirtumai tarp skirtingų miestų ir valstijų pačiose JAV įvairuoja. Kaip kraštutinį draudimų atvejį galima minėti Portlando miestą (Oregono valstija), kur egzistuoja bene griežčiausios pasaulyje taisyklės – VA naudojimas čia draudžiamas ne tik viešose vietose, bet ir privataus verslo (žmonių lankomose) erdvėse[48].

---

46 Kashmir Hill, „Wrongfully Accused by an Algorithm“, *The New York Times* (2020 m. rugpjūčio 3 d.), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

47 Tawana Petty, „Defending Black Lives Means Banning Facial Recognition“, *wired.com* (2020 m. spalio 7 d.), https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/.

48 Dave Gershgorn, „The Facial Recognition Backlash is Here. But will the current Bans Last?“, *onezero.medium* (2020 m. gruodžio 18 d.), https://onezero.medium.com/the-facial-recognition-backlash-15b5707444f3.

Daug kitų JAV miestų, panašiai kaip ir kai kurios privačios bendrovės, VA technologijai tiesiog paskelbė moratoriumą[49]. O kalbant apie platesnę biometrinių duomenų apsaugą, pasaulio žiniasklaidoje neretai cituojamas (kaip sektinas) JAV Ilinojaus valstijos Biometrinės nuosavybės įstatymas. Šis įstatymas traktuojamas kaip išsamiausias valstybės mastu kol kas nereguliuojamo skaitmeninio sekimo būdų (kartu ir VA) reguliavimo dokumentas[50]. Nors skirtingi gyventojų apklausų rezultatai JAV dėl VA naudojimo policijoje, mokyklose ar prekybos centruose taip pat rodo įvairias tendencijas, daugumai atrodo svarbu bent jau viešai iš(si)aiškinti mums nematomų, tačiau kasdienį mūsų gyvenimą administruojančių VA sistemų klaidas ir galimus pavojus[51]. Precedentai lėmė, kad ir IKT neutralumo tezė, kurią kai kurie tyrėjai siejo su kompiuterių mokslų pasiekimais, JAV sulaukė daugiausia tiek mokslininkų, tiek žiniasklaidos, pilietinės visuomenės institutų ar kai kurių politikų kritikos.

3.2. ES (ne)apsisprendimas pasauliniame kontekste

Šiais klausimais besidominčiose Europos šalyse, panašiai kaip ir kitur, diskutuojama apie DI sistemų skaidrumą, politiniuose pareiškimuose skelbiama, kad klasifikuojantys ir profiliuojantys algoritmai būtų „paaiškinami“ ir „skaidrūs“. Teisėkūroje visų pirma atsižvelgiama į 2018 m. įsigaliojusį Bendrąjį Europos duomenų apsaugos reglamentą; savo ruožtu naujai kuriamų ES dokumentų apžvalgose neretai pristatomas ir „europietiškas“ požiūris į VA[52], atskleidžiamas didėjantis

---

49 Kai kurios reputaciją siekiančios saugoti *Big Tech* bendrovės (IBM, „Amazon“ ir „Microsoft“) laikinai sustabdė VA įrangos pardavimus policijos departamentams ir, kaip minėta, skatino centrinės valdžios institucijas kuo greičiau kurti reguliacinę terpę (tačiau lygia greta daugybė kitų bendrovių toliau taiko VA technologiją). Žr. Julia Horowitz, „Tech Companies are still helping Police scan Your Face“, *CNN Business* (2020 m. liepos 3 d.), https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html.

50 Plačiau apie Ilinojaus įstatymus žr. Zuboff, 2019, 262.

51 Dave Gershgorn, „We Need to Know How Often Facial Recognition Fails“, *onezero.medium* (2020 m. birželio 26 d.).

52 „Veido atpažinimo technologijos – europietiško požiūrio formavimo procesas“, *Teise.pro* (2021 m. vasario 28 d.), https://www.teise.pro/index.php/2021/02/28/veido-atpazinimo-technologijos-europietisko-poziuro-formavimo-procesas/.

„europietiškos“ politikos skepsis dėl masinio darbuotojų stebėjimo[53]. Iš principo ES požiūrį į VA technologiją, ko gero, tikslinga vertinti ne tiek JAV egzistuojančių baimių dėl rasinio profiliavimo ar neteisingo juodaodžių suėmimo bei socialinio neteisingumo kontekste, kiek pasaulinės konkurencinės kovos ir inovacijų proveržio akivaizdoje.

Taigi turint mintyje pirmiau išsakytus klausimus, 2019–2020 m. ES institucijos ir pareiškimai dėl sekimo technologijų politikos plėtros iliustravo dvejones, neapsisprendimą, taip pat IKT verslo lobistų pastangas. Pavyzdžiui, emocijų atpažinimui naudojami įrenginiai buvo pristatomi kaip siekiamybė (kai kuriais atvejais ir jau kaip egzistuojanti realybė) Europos Komisijos 2019 m. parengtoje ekspertinėje ataskaitoje „100 radikalių inovacinių proveržių ateičiai“, kur kalbama apie pažangiuosius tyrimus, orientuotus į tobulesnes, nei dabar taikomos, VA, emocinių išraiškų šifravimo programas ir pagerintus melo detektorius[54]. 2020 m. sausio pradžioje Europos Komisija pasiūlė VA technologijos moratoriumą mažiausiai penkeriems ateinantiems metams (išskyrus saugumo ir mokslinių tyrimų sritis)[55]. Tačiau to paties mėnesio pabaigoje ES institucijos atsisakė ankstesnio sumanymo drausti VA viešose vietose[56].

O štai Europos Taryba jau 2021 m. sausį pasisakė prieš VA technologijos taikymą darbo rinkoje, neigiamai vertinta galimybė darb-

---

53 „Europarlamentarai: dirbtinis intelektas neturėtų būti naudojamas masiniam stebėjimui“, *Europos Parlamentas* (2021 m. spalio 6 d.), https://www.europarl.europa.eu/news/lt/press-room/20210930IPR13925/ep-dirbtinis-intelektas-neturetu-buti-naudojamas-masiniam-stebejimui.

54 „100 Radical Innovation Breakthroughs for the Future“, European Commission, Directorate-General for Research and Innovation (Luxembourg: Publications Office of the European Union, 2019), 87–89.

55 Daniel Boffey, „The EU might Temporarily ban Face Recognition in Public Places“, *The Guardian* (2020 m. sausio 17 d.), https://www.technologyreview.com/f/615068/facial-recognition-european-union-temporary-ban-privacy-ethicsregulation/?utm_source=newsletters&utm_medium=email&utm_campaign=the_algorithm.unpaid.engagement.

56 Foo Yun Chee, „EU drops Idea of Facial Recognition ban in Public Areas“ (2020 m. sausio 30 d.), https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q?fbclid=IwAR0E4_jmW543Zkc-Tv-H2jDAgVZo9GYEG-3qzfyok-BB-sIRrQhhy2isBvMo.

daviams be darbuotojų sutikimo matuoti asmens bruožus ir emocinį įsitraukimą į užduotis. Kaip teigiama parengto įstatymo projekte, DI šališkumo grėsmė naudojant VA kyla ne tik darbovietėje ar priimant į darbą, bet ir edukacinėje sistemoje, policijoje, teikiant draudimo paslaugas ir pan. Tapo akivaizdu, kad tobulėjančios vizualiosios kontrolės technologijos ir sekimas darbe kelia žmonėms emocinį diskomfortą, be to, jos gali būti diskriminuojančios bei pažeidžiančios asmens duomenų privatumą[57]. 2021 m. liepą ES duomenų apsaugos institucijos ragino visiškai uždrausti DI naudojimą automatiniam atpažinimui[58]. 2021 m. spalį Europos Parlamentas priėmė neįpareigojančią rezoliuciją, kurioje raginama uždrausti teisėsaugos institucijoms naudoti VA viešose vietose[59]. Rezoliucijoje taip pat siūloma paskelbti moratoriumą išankstinės prognozės įrankiams policijos programinėje įrangoje, apriboti nuotolinį biometrinio atpažinimo naudojimą, išskyrus kovos su „itin sunkiais“ nusikaltimais atvejais. Kadangi ES, skirtingai nei JAV, šiuo metu nėra aktualūs neteisingi suėmimai ar šiurkštūs algoritmų „apsirikimai“ ir diskriminacija dėl VA socialinėje politikoje (t. y. kivirčus įžiebiančių skandalų kol kas praktiškai nebuvo), pilietinės organizacijos ar žiniasklaida taip pat nekelia aštrių šio pobūdžio klausimų.

3.3. Lietuvos miestų gyventojus tyliai stebinti „kiniška akis“

Lietuvoje, kaip ir kitur, institucijos viešai neskelbia apie miestų erdvėse, viešojo ir privataus sektorių patalpose, prekybos vietose ar

---

57 Michael Peel ir Javier Espinoza, „Companies must not use Facial Recognition to Judge Staff, says Council of Europe“, *Financial Times* (2021 m. sausio 27 d.), https://www.ft.com/content/b83354dd-71bf-4feb-ad4a-461fb31aebe3.

58 „Europe Makes the Case to Ban Biometric Surveillance“, *Daloop* (2021 m. liepos 12 d.).

59 Melissa Heikkila, „European Parliament calls for a ban on Facial Recognition. Non-binding Resolution also asks for AI-based Predictive policing Ban“, *Politico* (2021 m. spalio 6 d.), https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/.

interneto priežiūros sistemose įdiegtas skaitmeninio sekimo ir biometrinių duomenų rinkimo technologijas, tačiau fragmentiški pranešimai žiniasklaidoje, kaip ir kai kurie pasisakymai, rodo, kad populiacijos stebėjimo, administravimo ir identifikavimo procese VA technologija užima svarbią vietą. Nesunku numanyti, jog pritarimas VA technologijai skamba DI įrankių kūrėjų lūpose. Populiariojoje juos cituojančioje žiniasklaidoje VA taip pat pristatomas kaip nekvestionuotinas saugumo garantas. Taigi visuomenė raginta šią technologiją kuo greičiau ir plačiau adaptuoti viešojoje politikoje[60]. Dėl galimų asmens privatumo pažeidimų plačiau nediskutuota (kartais minimas BDAR). Pirmiau tekste minėtieji teorinio ir etinio pobūdžio klausimai, kaip antai – ar iš tiesų žmogų geriausia analizuoti tada, kai pats individas pažinimo proceso negali nei matyti, nei suvokti – tarsi pakimba ore. Lietuvos DI tyrėjų ar panašių sričių akademikų darbuose šie klausimai arba lieka paraštėse, arba yra apeinami, mat duomenis analizuojantys mokslininkai į kompiuterinio matymo technologiją mieliau žvelgia kaip į neutralią matematinio skaičiavimo priemonę.

Kalbant apie optimistinės komputacinio empiricizmo retorikos atvejus galima minėti fragmentiškus bandymus tirti praeivius ir tai, kaip šie bandymai pristatyti Lietuvos viešojoje žiniasklaidos erdvėje. Pavyzdžiui, 2020-ųjų išvakarėse Vilnius žaismingai paskelbė, kad mieste įrengtomis kameromis stebėdamas vilniečius „VGTU mokslininkas kuria laimės formulę“[61]. Projekto vadovas Artūras Kaklauskas patikino, kad „asmeniniai duomenys nerenkami, sistema skaičiuoja nuasmenintus valandinius praeivių nuotaikų ir kitų duomenų vidurkius“. Vis dėlto kai automatizuoto klasifikavimo proce-

[60] Pasak Dovydo Vitkausko, Lietuvoje „galėtume pilotuoti ir patį efektyviausią ateities būdą identifikuoti asmenį pagal veido atpažinimo sistemą – FRS“. Žr. Dovydas Vitkauskas, „Galimybių pasą turėtų keisti veido atpažinimo sistema“, *delfi.lt* (2021 m. spalio 7 d.), https://www.delfi.lt/verslas/nuomones/dovydas-vitkauskas-galimybiu-pasa-turetu-keisti-veido-atpazinimo-sistema.d?id=88361491.

[61] Ernestas Naprys, „VGTU mokslininkas kuria laimės formulę – eksperimente kameromis stebimi vilniečiai“, *15min.lt* (2019 m. gruodžio 19 d.), https://www.15min.lt/verslas/naujiena/finansai/vgtu-mokslininkas-kuria-laimes-formule-eksperimente-kameromis-stebimi-vilnieciai-662-1250776?copied.

se nelieka jokio sąmoningo žmogaus apsisprendimo („čia apklausos nereikia. <…> čia gaunasi neuroapklausa, kai pati žmogaus kūno kalba užpildo visus klausimynus, ar tau gerai ar tau blogai yra“[62]), anoniminė technokratinė galia arba, Zuboff žodžiais tariant, *Didysis Kitas* pasilieka išimtinę teisę matematiškai analizuoti žmones ir kurti „laimės formules“ apie vizualiąją kontrolę nė neįtariančiai visuomenei. Šį tiriamojo žmogaus ne(be)dalyvavimą, individo kaip subjekto „išnykimą“ kaupiant iš tų pačių individų gaunamus duomenis[63] galima sieti su etiniu požiūriu gana dviprasmiškomis socialinėmis ir biopolitikos iniciatyvomis. „Aplinką matanti mašina“ gali nematomai atlikti „neuroapklausą“, o kadangi įsivaizduojama, jog mašinos mus „geriausia nuskaito“ tada, kai eliminuojamas subjekto intencionalumas, automatizuoto žmonių klasifikavimo procesas „nejučia“ ima tarnauti grynajam instrumentalizmui.

Tačiau vizualiosios kontrolės grėsmės Lietuvos žiniasklaidoje nevienprasmiškai minimos tada, kai kyla įtarimas dėl šalies saugumo. T. y. kai paaiškėja, kad vietinės institucijos naudojasi autoritarinių šalių tiekiama programine įranga. Ne sykį nuogąstauta, jog Lietuvoje taikoma Kinijoje kurta VA technologija – pavyzdžiui, 2020 m. sausį skelbta, jog Kaune gyventojus stebi kiniškos kameros (fiksuojančios veidus ir eismo pažeidimus), kurių dėl saugumo atsisakyta JAV[64]. Beje, minėta ir tai, kad JAV atsisakius specifinių su sekimu skaitmeninėje erdvėje ir šiurkščiais žmogaus teisių pažeidimais siejamų kinų

---

62 Made in Vilnius, „Mokslininkai Vilniaus gatvėse matuoja praeivių emocijas, temperatūrą bei kvėpavimo dažnį“, *delfi.lt* (2019 m. gruodžio 24 d.), https://www.delfi.lt/miestai/vilnius/mokslininkai-vilniaus-gatvese-matuoja-praeiviu-emocijas-temperatura-bei-kvepavimo-dazni.d?id=83040699&fbclid=IwAR1HCSXaPvthcc_VG6asgaK7RJDMuJ13npZ2tESrZCjLepAR43_hJWsAYp8.

63 Iš etinės perspektyvos tokias iniciatyvas kritiškai vertinau rašydama apie (dar tik kuriamus) lietuviškuosius emocijų atpažinimo įrankius, tokius kaip valstybės institucijų siūlomas „Jausmomatis“. Žr. Trilupaitytė, 2020.

64 Paulius Vaitekėnas, „Kaune gyventojus stebi žmonių sekimu pagarsėjusios kinų kameros: fiksuos žmonių veidus ir KET pažeidimus“, *LRT.lt.* (2020 m. sausio 29 d.), https://www.lrt.lt/naujienos/eismas/7/1137677/kaune-gyventojus-stebi-zmoniu-sekimu-pagarsejusios-kinu-kameros-fiksuos-zmoniu-veidus-ir-ket-pazeidimus?fbclid=IwAR1VKjHQEWAWLVo3d5IJJpvYCv09ZLlgovZtkGpfAJPiaLvFIgMxA23HFM0.

bendrovių („Hikvision“ ir „Dahua“) paslaugų, Lietuvoje šių bendrovių produktai yra toliau perkami. Neva itin didelę patirtį VA technologijų ir duomenų apdorojimo srityse sukaupusių Kinijos bendrovių „kameromis naudojasi bent šešios jautrią informaciją kaupiančios valstybės institucijos“[65].

Taigi, nors ir baiminamasi grėsmingos „kiniškos akies“ miestų erdvėse, iš viešai cituojamų pareigūnų ir už duomenų apsaugą atsakingų institucijų atstovų pasisakymų žiniasklaidoje nėra aišku, ką konkrečiai kameros stebi, kokie duomenys (ne)renkami ir kaip jie vėliau saugomi. Vieša retorika tiesiog išduoda nematomą įtampą tarp vizualiosios kontrolės (teisėto) naudojimo ir ES privačių duomenų apsaugos įstatymų (galimo) nesilaikymo[66]. Kitaip tariant, vizualioji kontrolė didžiuosiuose Lietuvos miestuose yra reali, tačiau šią nematomą kontrolę gaubia ir savotiškas „nežinojimo“ režimas. VA galimybės, kaip ir kitur, susiejamos su saugumo naratyvais (tai – įprasti *Big Tech* bendrovių aiškinimai apie išankstinį nusikaltimų užkardymą, hipotetinę galimybę rasti dingusius žmones, saugumą keliuose, pandemijos valdymą). Tačiau šie naratyvai kontrastuoja su nuogąstavimais, jog kai kurie IKT sprendimai, pasitelkiant autoritarinės šalies įrangą, saugumą ne didina, o mažina. Apskritai tikėtina, kad Lietuvoje VA ir kitas biometrinio sekimo technologijas ilgainiui reglamentuos ne savivaldos institucijos, bet platesni ES teisiniai reikalavimai ir savitai VA technologijai kuriami įstatymai.

---

65 Minėtas kameras Lietuvos institucijos įsigijo 2017–2019 m. Žr. „Lietuvos vadovus saugo kameros, kurių bijo amerikiečiai“, *LRT tyrimai* (2020 m. sausio 29 d.), https://www.lrt.lt/naujienos/lrt-tyrimai/5/1137518/lrt-tyrimas-lietuvos-vadovus-saugo-kameros-kuriu-bijo-amerikieciai?fbclid=IwAR2Y9BLDthGBeGX4RrNa9v0zrDww6E3myMXU0iJFwJELIPTbe8znM-mVaKY.

66 Valdemaras Šukšta, „Kiniška akis“ Kaune: nors palaiminimo miesto gatvėse naudoti kameras dar negauta, policija tyliai jas jau išmėgina“, *LRT.lt* (2021 m. lapkričio 19 d.), https://www.lrt.lt/naujienos/lietuvoje/2/1541495/kiniska-akis-kaune-nors-palaiminimo-miesto-gatvese-naudoti-kameras-dar-negauta-policija-tyliai-jas-jau-ismegina.

Pabaigai

Vizualiosios kontrolės šiandienos visuomenėse stiprėjimas, grėsmės ir ateities galimybės puikiai atsiskleidžia analizuojant VA technologiją gaubiančias šiandienos IKT inovacijų prieštaras. Kalbant tiek apie naujų įrankių įgalintą žmonių sekimą realiu laiku, tiek apie kylantį vis didesnį pasipriešinimą kontrolei ir asmens privatumo nykimui, galima stebėti du lygiagrečius procesus. Viena vertus, technologijų pažangą ir efektyvų taikymą kasdienybėje spartina dideles duomenų bazes gebančios apdoroti skaičiavimo mašinos ir kasdien tobulinti algoritmai. VA technologijos efektyvumas tarsi natūraliai įkvepia ir pirmenybės technologiniams sprendimams viešojoje politikoje teikimui (*technosolutionism*), tam implicitiškai pasitelkiama technologijų neutralumo nuostata. Kita vertus, dėl padidėjusių VA galimybių technologija tampa ir savotiška grėsme. Iš principo, technooptimizmas, kaip ir technopesimizmas, gali būti traktuojami tarsi dvi moderniosios vakarietiškos technologinės kultūros medalio pusės, tačiau šiandien tikslinga kalbėti ne tik apie minėtąją (tradicinę) perskyrą, bet ir apie tam tikrų abejonių keliančias ideologines tiksliųjų mokslų prielaidas. Kai kurie pastarųjų metų užsienio žiniasklaidoje plačiai cituojami šiame tekste minėti VA poveikio JAV tyrimai rodė, kad technologija nėra pati savaime neutrali, nes iš šalies nematomo vizualiojo sekimo ir administravimo rezultatai yra prisodrinti mašininio mokymo algoritmų kūrėjų ir naudotojų sąmoningų bei nesąmoningų intencijų. Tradiciškai technikos filosofijoje apsvarstoma „dviašmenė“ inovacijų prigimtis, kai dinamiškoje taikomojo mokslo realybėje teigiamą poveikį sunku vienprasmiškai atskirti nuo neigiamo, atsikartoja ir svarstymuose apie VA. Juk gali nutikti taip, kad totalinio sekimo kapitalizmo režimą steigianti IKT inovacija, pasiekusi savo apogėjų, bus šalinama iš viešojo gyvenimo. Nors tam tikros technologijos visuomenėje kažkada radosi kaip svarbi taikomoji mokslo pažangos proceso dalis, jų naudojimas vėliau maksimaliai užkardytas (atominės bombos gamyba, plutonio atliekų naudojimas ir pan.)

Pilietinės visuomenės institutų ataskaitos rodo, kad naujomis sekimo galimybėmis, nepaisant viešų deklaracijų, galiausiai pasinaudoja galios režimai (ar tai būtų Kinija, JAV, ar kitos šalys). O anoniminė algoritminė valdysena neatsiejama nuo (diskriminacinių) administravimo procesų ar populiacijų valdymo. Vizualiosios kontrolės įrankiais galios institucijos visada yra linkusios pasinaudoti, ypač jei tokių įrankių naudojimas nėra aiškiau reglamentuotas, o pati technologija nėra griežtai reguliuojama teisiškai. Nors vizualioji kontrolė ir gali būti siejama su vis tikslesnėmis biopolitikos priemonėmis valdant pasaulinę pandemiją ir steigiant viešosios erdvės saugumo režimus, tenka pripažinti, jog greit plintantys sofistikuoti matymo įrenginiai neabejotinai turi savo tamsiąsias puses. Apie pastarąsias šiandien kalba ne tik žmogaus teisių aktyvistai, bet ir patys DI srities technologijų ekspertai, įmonių vadovai, taip pat akademiniai tyrėjai (visų pirma JAV).

Galima netgi teigti, kad būtent JAV atvejai ir viešai aptariami pastarųjų metų precedentai ženklina naują pasaulinį frontą pilietinės visuomenės atstovams kovojant dėl (skaitmenizuotų) politinių sprendimų skaidrumo ir aiškinantis apie DI sistemų šalutinį poveikį. DI juodoji dėžė klasifikuoja ir netgi įvertina žmones – vartotojus, pirkėjus, mokinius, darbuotojus, nusikaltėlius etc. – pagal patiems žmonėms nesuvokiamą „matematinę logiką“. O pirmenybės šiai logikai teikimas viešojoje politikoje, t. y. įsivaizdavimas, jog matematinių algoritmų apdorojami duomenys ir predikcijos modelius kuriančios sistemos įgalina „objektyvesnį“ tikrovės vaizdą, provokuoja akylesnį žvilgsnį ir į technikos ideologizavimą. JAV sparčiai besiplėtojanti VA ir automatizuoto atpažinimo bei sekimo sistema paskatino būtent šios šalies tyrėjus ekspertus užimti kur kas kritiškesnę poziciją analizuojant plataus technologijų taikymo pasekmes.

Kadangi VA pasitelkiamas patiems įvairiausiems tikslams – nuo greitesnio personalizuoto aptarnavimo, pavyzdžiui, akimirksniu identifikuojant veidą ir vartotojui suteikiant unikalią prieigą prie paslaugų, iki to paties veido savininko nuolatinio sekiojimo, profiliavimo ir net (nematomos) diskriminacijos – veidų atpažinimo tobuli-

nimas nereiškia „užtikrinto saugumo“. Dėl žiniasklaidoje paviešintų nemalonių precedentų technologija sulaukia gana aršaus pasipriešinimo demokratines tradicijas turinčiose visuomenėse. Nuogąstavimus šiandien kelia ir lengvai prieinamos VA programėlės galimų individualių nusikaltėlių rankose (personalizuota neinstitucinio asmens persekiojimo grėsmė, žinoma, jau būtų platesnė tema). Savo ruožtu, žmonių analitikoje naudojamas veidų stebėjimas ir automatizuotas asmens emocijų, būsenų ar vidinių intencijų, etninės priklausomybės ar seksualinės orientacijos atpažinimas pasitelkiant matematinius modelius taip pat kelia pagrįstų abejonių.

Taigi, viena vertus, tiksliųjų, gamtos ir socialinių mokslų sankirtose ilgainiui susiformavęs tam tikras žinojimo diskursas skatina VA ir panašių priemonių kūrėjus rasti vis naujesnių būdų, kaip eliminuoti žmogaus subjektyvumą ir, pasitelkiant sekimo technologijas, pasiekti kuo objektyvesnį sociumo ir individų pažinimą (tai siejasi su filosofinėmis „technologijos neutralumo“ tezėmis). Kita vertus, manymas, jog mašina gali geriau „matyti“ ir pažinti žmogų nei pats žmogus, sulaukia nevienprasmiškos kritikos. Skirtingose šalyse įstatymai ir VA technologijos taikymą apibrėžiantys reglamentai dar tik kuriami, taigi ir pragmatiniu lygmeniu kol kas nėra universalaus atsakymo dėl asmens veido duomenų panaudojimo ir saugojimo. JAV daugiausia priešinamasi vizualiosios kontrolės bei sekimo priemonėms; VA technologijos reputacija šioje šalyje smuko ir dėl algoritmų šališkumą atskleidusių akademinių tyrimų. Savo ruožtu, kadangi JAV būdingi nesusipratimai dėl rasinio profiliavimo socialinėje sferoje ar neteisingo suėmimo naudojantis VA technologija ES šiuo metu faktiškai neegzistuoja, čia šiuo metu siekiama konkuruoti pasaulio mastu dėl IKT inovacijų, kartu ir dėl VA. Didėjantis vakarietiškų šalių visuomenių technosąmoningumas taip pat koreliuoja su didėjančiu žmonių poreikiu išlikti neatpažintiems „mašinos akies“. Vis dėlto tai, ar pasaulyje įsigalės distopinis sekimo kapitalizmo variantas, ar teisę į žmogaus individualumą, privatumą ir subjektyvų (ne)neapsisprendimą apsauganti sistema, kol kas lieka ateities klausimas.

Literatūra

Alba, Davey ir Villa Lissandra. „As Concerns Over Facial Recognition Grow, Members of Congress are Considering Their Next Move“. *buzzfeednews.com* (2019 m. vasario 20 d.). https://www.buzzfeednews.com/article/daveyalba/house-oversight-committee-hearing-facial-recognition

„As Face-recognition Technology Spreads, so do Ideas for subverting It“. *economist.com* (2019 m. rugpjūčio 15 d.). https://www.economist.com/science-and-technology/2019/08/15/as-face-recognition-technology-spreads-so-do-ideas-for-subverting-it.

Buolamwini, Joy ir Timnit Gebru. „Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification“. *Proceedings of Machine Learning Research* (PMLR'18), 1–15 (New York, 2018).

Bronstein, Hugh. „Rights Group criticizes Buenos Aires for Using Face Recognition Tech on Kids“. *Reuters* (2020 m. spalio 9 d.). https://www.reuters.com/article/uk-argentina-rights-idUKKBN26U208.

Bogert, Eric, Aaron Schecter ir Richard T. Watson. „Humans rely More on Algorithms Than Social Influence as a Task becomes More Difficult“ (2021). *Scientific Reports.* https://www.nature.com/articles/s41598-021-87480-9.

Boffey, Daniel. „The EU might Temporarily ban Face Recognition in Public Places“. *The Guardian* (2020 m. sausio 17 d.). https://www.technologyreview.com/f/615068/facial-recognition-european-union-temporary-ban-privacy-ethicsregulation/?utm_source=newsletters&utm_medium=email&utm_campaign=the_algorithm.unpaid.engagement.

Burges, Matt. „Some UK Stores are using Facial Recognition to track Shoppers“. Žiūrėta 2020-12-20. www.wired.com.

Campbell, Ian. „Moscow adds Facial Recognition Payment System to More Than 240 Metro Stations“. *The Verge* (2021 m. spalio 15d.). www.theverge.com/2021/10/15/22728667/russia-face-pay-system-moscow-metro-privacy.

Campolo, Alexander ir Kate Crawford. „Enchanted Determinism: Power without Responsibility in Artificial Intelligence“. *Engaging Science, Technology, and Society* Vol. 6 (2020). DOI: https://doi.org/10.17351/ests2020.277.

Couldry, Nick ir Ulises Mejias. „The Decolonial Turn in Data and Technology Research: What is at stake and where is It Heading?“. *Information, Communication & Society* (2021, Nov 9). https://doi.org/10.1080/1369118X.2021.1986102.

Chee, Foo Yun. „EU drops Idea of Facial Recognition ban in Public Areas“ (2020 m. sausio 30 d.). https://www.reuters.com/article/us-eu-ai/eu-drops-idea-of-facial-recognition-ban-in-public-areas-paper-idUSKBN1ZS37Q?fbclid=IwAR0E4_jmW543ZkcTv-H2jDAgVZo9GYEG-3qzfyok-BB-sIRrQhhy2isBvMo.

Christian, Jon. „How Facial Recognition could tear us Apart“. *onezeromedium.com* (2018 m. rugsėjo 17 d.).

Crawford, Kate ir Trevor Paglen. „Excavating AI. The Politics of Images in Machine Learning Training Sets for Machine Learning“. Žiūrėta 2019-09-19. https://www.excavating.ai/.

„Dirbtinio intelekto valdomą parduotuvę sukūrusiam lietuvių startuoliui – milijono eurų investicija“. *15min.lt.* (2020 m. rugpjūčio 5 d.). https://www.15min.lt/verslas/naujiena/bendroves/dirbtinio-intelekto-valdoma-parduotuve-sukurusiam-lietuviu-startuoliui-milijono-euru-investicija-663-1357492?copied&copied.

Douglas, W. Heaven. „Predictive policing Algorithms are Racist. They Need to be dismantled“. *MIT Technology Review* (2020 m. liepos 17 d.). https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

„Europarlamentarai: dirbtinis intelektas neturėtų būti naudojamas masiniam stebėjimui“. *Europos Parlamentas* (2021 m. spalio 6 d.). https://www.europarl.europa.eu/news/lt/press-room/20210930IPR13925/ep-dirbtinis-intelektas-neturetu-buti-naudojamas-masiniam-stebejimui.

„Europe Makes the Case to Ban Biometric Surveillance“. *OODaloop* (2021 m. liepos 12 d.). https://www.oodaloop.com/briefs/2021/07/12/europe-makes-the-case-to-ban-biometric-surveillance/.

Gershgorn, Dave. „Aggression Detection' is Coming to Facial Recognition Cameras Around the World“. *onezero.medium* (2020 m. rugsėjo 25 d.). https://onezero.medium.com/aggression-detection-is-coming-to-facial-recognition-cameras-around-the-world-90f73ff65c7f.

Cho Mu-Hyun. „Seoul to install AI Cameras for Crime Detection“. *ZDNet* (2020 m. sausio 2 d.). https://www.zdnet.com/article/seoul-to-install-ai-cameras-for-crime-detection/.

Gershgorn, Dave. „We Mapped How the Coronavirus is Driving New Surveillance Programs Around the World“. *onezero.medium* (2020 m. balandžio 9 d.). *https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9.*

Gershgorn, Dave. „The U.S. Fears Live Facial Recognition. In Buenos Aires, it's a Fact of Life“. *onezero.medium* (2020 m. kovo 4 d.). https://onezero.medium.com/the-u-s-fears-live-facial-recognition-in-buenos-aires-its-a-fact-of-life-52019eff454d.

Gershgorn, Dave. „The Facial Recognition Backlash is Here. But will the current bans last?“. *onezero.medium* (2020 m. gruodžio 18 d.). https://onezero.medium.com/the-facial-recognition-backlash-15b5707444f3.

Gershgorn, Dave. „We Need to Know How Often Facial Recognition Fails“. *onezero.medium* (2020 m. birželio 26 d.). https://onezero.medium.com/we-need-to-know-how-often-facial-recognition-fails-e9ba3a90745f.

Goldenfein, Jake. „Facial Recognition is Only the Beginning“. *Public Books* (26 Mar 2020). https://ssrn.com/abstract=3546525.

Hartzog, Woodrow. „Facial Recognition is the Perfect Tool for Oppression“. *medium.com* (2018 m. rugpjūčio 2 d.). https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66.

Heaven, W. Douglas. „Predictive policing Algorithms are Racist. They Need to be dismantled“ (2020 m. liepos 17 d.). *MIT Technology Review*, https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

Heikkila, Melissa. „European Parliament calls for a ban on Facial Recognition. Non-binding Resolution also asks for AI-based Predictive policing Ban“. *Politico* (2021 m. spalio 6 d.). https://www.politico.eu/article/european-parliament-ban-facial-recognition-brussels/.

Hill, Kashmir. „Wrongfully Accused by an Algorithm“. *The New York Times* (2020 m. rugpjūčio 3 d.). https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.

Horowitz, Julia. „Tech Companies are still helping Police scan Your Face“. *CNN Business* (2020 m. liepos 3 d.). https://edition.cnn.com/2020/07/03/tech/facial-recognition-police/index.html.

„Lietuvos vadovus saugo kameros, kurių bijo amerikiečiai“. *LRT tyrimai* (2020 m. sausio 29 d.). https://www.lrt.lt/naujienos/lrt-tyrimai/5/1137518/lrt-tyrimas-lietuvos-vadovus-saugo-kameros-kuriu-bijo-amerikieciai?fbclid=IwAR2Y9BLDthGBeGX4RrNa9v0zrDww6E3myMXU0iJFwJELIPTbe8znM-mVaKY.

Made in Vilnius. „Mokslininkai Vilniaus gatvėse matuoja praeivių emocijas, temperatūrą bei kvėpavimo dažnį“. *delfi.lt* (2019 m. gruodžio 24 d.). https://www.delfi.lt/miestai/vilnius/mokslininkai-vilniaus-gatvese-matuoja-praeiviu-emocijas-temperatura-bei-kvepavimo-dazni.d?id=83040699&fbclid=IwAR1HCSXaPvthcc_VG6asgaK7RJDMuJ13npZ2tESrZCjLepAR43_hJWsAYp8.

Morozov, Evgeny. *To Save Everything, Click Here: The Folly of Technological Solutionism.* New York: Public Affairs, 2014.

Murgia, Madhumita. „Who’s Using Your Face? The Ugly Truth about Facial Recognition“. *Financial Times* (2019 m. balandžio 19 d.). https://www.ft.com/content/cf19b956-60a2-11e9-b285-3acd5d43599e.

Naprys, Ernestas. „VGTU mokslininkas kuria laimės formulę – eksperimente kameromis stebimi vilniečiai“. *15min.lt* (2019 m. gruodžio 19 d.). https://www.15min.lt/verslas/naujiena/finansai/vgtu-mokslininkas-kuria-laimes-formule-eksperimente-kameromis-stebimi-vilnieciai-662-1250776?copied.

Kalpokas, Ignas. *Algorithmic Governance: Politics and Law in the Post-Human Era*. Cham: Palgrave Macmillan, 2019.

O'Neil, Cathy. *Weapons of Math Destruction.* New York: Crown Books, 2016.

Peel, Michael ir Javier Espinoza. „Companies must not use Facial Recognition to Judge Staff, says Council of Europe". *Financial Times* (2021 m. sausio 27 d.). https://www.ft.com/content/b83354dd-71bf-4feb-ad4a-461fb31aebe3.

Petty, Tawana. „Defending Black Lives Means Banning Facial Recognition". *www.wired.com* (2020 m. spalio 7 d.). https://www.wired.com/story/defending-black-lives-means-banning-facial-recognition/.

United States Department of Commerce. Privacy Multistakeholder Process: Facial Recognition Technology (2016 m. birželio 17 d.). National Telecommunications and Information Administration. https://www.ntia.doc.gov/other-publication/2016/privacy-multistakeholder-process-facial-recognition-technology.

Ropohl G. „Ropol G.: Techninis problemų sprendimas". In *Technikos filosofijos įvadas*. Vilnius: Kultūros ir meno institutas, 1998.

Rouvroy, Antoinette ir Thomas Berns. „Algorithmic Governmentality and Prospects of Emancipation. Disparateness as a Precondition for Individuation through Relationships?" (Translated by Elizabeth Libbrecht). *Réseaux*, Vol. 177, Issue 1 (2013): 163–196.

Rushkoff, Douglas. *Team Human.* WW. Norton & Company, New York: 2019.

„Schools adopt Face Recognition in the Name of Fighting Covid". *www.wired.com.* (2020 m. lapkričio 3 d.). https://www.wired.com/story/schools-adopt-face-recognition-name-fighting-covid/.

Smonite, Tom. „Facial Recognition is Suddenly Everywhere. Should You Worry?". *www.wired.com* (2019 m. birželio 8 d.). https://www.wired.com/story/facial-recognition-everywhere-should-you-worry/.

Smith, Adam. „The Met police's Decision to use Facial Recognition not Only harms our Right to Privacy – It damages Our Democracy, Too". *Prospect* (2020 m. vasario 3 d.). https://www.prospectmagazine.co.uk/science-and-technology/met-police-facial-recognition-london-kings-cross-bias-uk.

Smith, Brad. „Facial Recognition Technology: The Need for Public Regulation and Corporate Responsibility". *Microsoft on the Issues* (2018 m. liepos 13 d.). https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/.

Stark, Luke. „Facial Recognition is the Plutonium of AI". *XRDS* 25, nr. 3 (2019 Spring). DOI: 10.1145/3313129. https://static1.squarespace.com/static/59a34512c534a5fe6721d2b1/t/5cb0bf02eef1a16e422015f8/1555087116086/Facial+Recognition+is+Plutonium+-+Stark.pdf

Stiegler, Bernard. *Automatic Society, Vol 1. The Future of Work* (translated by D. Ross). Cambridge, Malden: Polity Press, 2016.

Šukšta, Valdemaras. „Kiniška akis“ Kaune: nors palaiminimo miesto gatvėse naudoti kameras dar negauta, policija tyliai jas jau išmėgina“. *lrt.lt* (2021 m. lapkričio 19 d.). https://www.lrt.lt/naujienos/lietuvoje/2/1541495/kiniska-akis-kaune-nors-palaiminimo-miesto-gatvese-naudoti-kameras-dar-negauta-policija-tyliai-jas-jau-ismegina.

Tangermann, Victor. „Could This Neural Network Really be better at predicting Personality Traits Than Humans?“. *Futurism* (2020 m. gegužės 22 d.). https://futurism.com/researchers-ai-judge-personality-selfies.

Trilupaitytė, Skaidra. „Protingas valdymas ir ekspertiniai laimės įrankiai“. *Kultūros barai*, nr. 5 (2020).

Trilupaitytė, Skaidra. „Spąstai žmogaus pasauliui“. *Athena: filosofijos studijos*, nr. 16 (2021).

Zuboff, Shoshana. „The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power“. *Public Affairs*, 2019.

Vaitekėnas, Paulius. „Kaune gyventojus stebi žmonių sekimu pagarsėjusios kinų kameros: fiksuos žmonių veidus ir KET pažeidimus“. *LRT.lt.* (2020 m. sausio 29 d.). https://www.lrt.lt/naujienos/eismas/7/1137677/kaune-gyventojus-stebi-zmoniu-sekimu-pagarsejusios-kinu-kameros-fiksuos-zmoniu-veidus-ir-ket-pazeidimus?fbclid=IwAR1VKjHQEWAWLVo3d5IJJpvYCv09ZLlgovZtkGpfAJPiaLvFIgMxA23HFM0.

„Veido atpažinimo technologijos – europietiško požiūrio formavimo procesas“. *Teise.pro* (2021 m. vasario 28 d.). https://www.teise.pro/index.php/2021/02/28/veido-atpazinimo-technologijos-europietisko-poziuro-formavimo-procesas/.

Vitkauskas, Dovydas. „Galimybių pasą turėtų keisti veido atpažinimo sistema“. *delfi.lt* (2021 m. spalio 7 d.). https://www.delfi.lt/verslas/nuomones/dovydas-vitkauskas-galimybiu-pasa-turetu-keisti-veido-atpazinimo-sistema.d?id=88361491.

Wang, Yilun ir Michal Kosinski. „Deep Neural Networks are More Accurate Than Humans at Detecting Sexual Orientation from Facial Images“. *Journal of Personality and Social Psychology* 114, nr. 2 (2018).

„100 Radical Innovation Breakthroughs for the Future“. European Commission, Directorate-General for Research and Innovation, 87–89. Luxembourg: Publications Office of the European Union, 2019.