DIRBTINIS INTELEKTAS IR DUOMENŲ APSAUGA KRIMINALISTIKOS PLĖTROS KONTEKSTE

Jurgita Baltrūnienė,
Statutinio ugdymo institutas,
Viešojo saugumo akademija, Mykolo Romerio universitetas,
Maironio g. 27, 44298 Kaunas, Lietuva,
Kauno apygardos prokuratūros
Kauno apylinkės prokuratūra, prokurorė,
Maironio g. 30, 44298 Kaunas, Lietuva,
<baltruniene.jurgita@gmail.com>

Anotacija

Straipsnyje analizuojama kaip dirbtinis intelektas (DI) keičia žmonių gyvenseną ir darbo būdą. Atsižvelgiant į sparčią DI technologijų plėtrą ir į pasaulinį politinį kontekstą, būtent į tai, kad vis daugiau šalių gausiai investuoja į DI, ES turi veikti išvien, kad perspektyviai išnaudotų daugybę DI teikiamų galimybių ir išspręstų jo keliamus uždavinius. Europos DI srities pajėgumų stiprinimas – labai svarbus elementas siekiant įgyvendinti platesnę strategiją, kurios tikslas – užtikrinti, kad Europa prisitaikytų prie skaitmeninio amžiaus ir kad, kaip nustatyta Skaitmeninės politikos kelrodžio komunikate, ateinantys 10 metų taptų skaitmeniniu dešimtmečiu. DI gali būti strateginė priemonė, suteikianti galimybę kovoti su esamomis grėsmėmis ir numatyti tiek būsimą riziką, įskaitant hibridines grėsmes, tiek galimybes. Taip pat gali padėti kovoti su nusikalstamumu ir terorizmu, sudaryti teisėsaugos institucijoms sąlygas sekti sparčią nusikaltėlių naudojamų technologijų raidą ir jų tarpvalstybinę veiklą. Mūsų manymu kriminalistikos atstovai dar nepakankamai dėmesio skiria šiai problematikai. Tai turi būti viena iš strateginių kriminalistikos plėtros krypčių. DI gali padėti siekti ES saugumo strategijos tikslų.

Raktiniai žodžiai: dirbtinis intelektas (DI), Europos Sąjungos vidaus saugumo strategija, asmens duomenys, apsauga, privatumas.

Įvadas

Dirbtinis intelektas (DI) nepaprastai veikia žmonių gyvenseną ir darbo būdą. Atsižvelgdama į sparčią DI technologijų plėtrą ir į pasaulinį politinį kontekstą, būtent į tai, kad vis daugiau šalių gausiai investuoja į DI, ES turi veikti išvien, kad perspektyviai išnaudotų daugybę DI teikiamų galimybių ir išspręstų jo keliamus uždavinius. Komisijos politiką, kurios pradžia – 2018m. balandžio

mėn. paskelbta Europos DI strategija[1], sudaro dvi kryptys: viena vertus, siekiama, kad ES taptų pasaulinio lygio DI centru, kita vertus, dedamos pastangos užtikrinti, kad DI būtų orientuotas į žmogų ir patikimas.

Šiuo straipsniu siekiama atkreipti dėmesį į DI keliais aspektais. Pirmuoju aspektu apžvelgiama dirbtinio intelekto samprata, jo veikimo principai, rūšys bei išanalizuotas svarbiausias šios dalies klausimas – teisinio statuso suteikimas dirbtiniam intelektui. Šiuo laikotarpiu, technologijų dėka sukurti produktai nėra laikomi tik žmonių pagalbininkais, tačiau vis dažniau kyla klausimas dėl jų autonomiškumo bei savarankiškumo. Šiame straipsnyje apžvelgiama, kas laikoma dirbtiniu intelektu teisine prasme ir kodėl jau netolimoje ateityje galima tikėtis susidurti su „elektroniniu asmeniu“, kuris išsiskirs nuo paprastų elektroninių priemonių savo autonomiškumu ir gebėjimu mąstyti, suvokti, priimti sprendimus, o svarbiausia – gebėjimu mokytis. Antruoju aspektu apžvelgiama asmenų teisės, kurios turi būti apsaugotos nuo dirbtinio intelekto daromo poveikio, būtent, bus apžvelgiamos tokios teisės ir laisvės, įtvirtintos pagrindiniuose tarptautiniuose ir Europos Sąjungos teisės aktuose, kaip: asmens teisė į duomenų apsaugą, privatumą, orumo garantavimą, draudimas diskriminuoti, teisė į teisingą teismą, ir kt. Išanalizavus šių teisių ir laisvių turinį, bus pateikti aktualiausi jų pažeidimo atvejai dirbtinio intelekto kontekste. Taip pat, bus atkreiptas dėmesys ir į atsakomybės klausimą, t. y. kas turi atsakyti už robotų, kaip fizinės dirbtinio intelekto išraiškos, padarytą žalą. Šiame kontekste bus analizuojamas esamas reguliavimas bei nagrinėjamas Europos Parlamento pateiktas pasiūlymas dėl Robotikos chartijos priėmimo Europos Sąjungos mastu, kurio pagalba siekiama sureguliuoti šį ir kitus toliau nagrinėjamus klausimus. Trečiuoju aspektu – kaip kriminalistikos mokslas ir jo strategija reaguoja į šiuos procesus?Norėdamas parodyti kriminalistikos mokslo reikšmę, H. Grossas rašė: „Kokiu būdu mes galim rasti tą ar kitą įrodymą, kaip prie jų prieiti, kaip juos apsaugoti ir panaudoti, visa tai taip pat svarbu, tai tas rezultatas, kurio mes siekiame vykdydami teisingumą. Rasti ir panaudoti nusikaltėlio pėdsakai, kruopščiai nubraižytas nors ir nesudėtingas brėžinys, mikroskopinis preparatas, iššifruotas susirašinėjimas, fotografinės nuotraukos, tatuiruotės, atkurtas apanglėjęs laiškas, koks nors tikslus matmuo ir tūkstančiai panašių realijų – tai ne kas kita, kaip nepaperkami liudytojai, neleidžiantys paneigti ir kartu leidžiantys nuolat tikrinti, liudytojai, kurių atžvilgiu negalima klaida, vienpusiškas supratimas, pikta valia, šmeižtas ir panašiai. Su kiekvienu

[1] Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos Ekonomikos ir Socialinių reikalų komitetui ir regionų komitetui. *Dirbtinis intelektas Europai* {SWD(2018) 137 final}; 2018 04 25 COM(2018) 237 final.

kriminalistikos laimėjimu krenta liudytojų parodymų reikšmė ir drauge kyla realių įrodymų reikšmė“[2]. Savo laiku, profesorius Hansas Grossas ir kiti kriminalistikos mokslo pradininkai pamatė būtinumą diegti gamtos ir technikos mokslų pasiekimus į nusikaltimų aiškinimo ir tyrimo procesus, kaip efektyvų kovos su nusikalstamumu įrankį. Mūsų laikais jau nestebina platus informacinių technologijų diegimas į kriminalistikos mokslą, o per jį, kriminalistikos rekomendacijų pavydalu į nusikaltimų aiškinimo ir tyrimo procesus. Žvelgiant į ateitį, mes privalome ne tik parengti strategines kriminalistikos plėtros kryptis, tame tarpe ir numatant DI galimybių panaudojimą, bet ir užsiimti taikomaisiais darbais, kurie leistų jau šiandien adaptuoti kitų sričių DI pasiekimus kovoje su nusikalstamumu.

Kas yra dirbtinis intelektas ir kaip jis veikia?

Dirbtinis intelektas – tai sistemos, kurios elgiasi protingai, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti. Dirbtinio intelekto sistemos gali būti grindžiamos vien tik programine įranga ir veikti virtualiajame pasaulyje (pvz., balso sintezatoriai, vaizdo analizės programinė įranga, paieškos sistemos, kalbos ir veido atpažinimo sistemos) arba gali būti integruotos techninėje įrangoje (pvz., pažangiuose robotuose, savaeigėse transporto priemonėse, bepiločiuose orlaiviuose ar daiktų interneto objektuose). Mes kasdien naudojame dirbtinį intelektą, pvz., versdami tekstus, kurdami vaizdo įrašų subtitrus ar blokuodami el. pašto šiukšles. Naujausias mokslo pasiekimas – dirbtinis intelektas, yra naujų kriminalistikos idėjų ir metodų, susijusių su jo naudojimu, kovojant su nusikalstamumu[3]. Daugumai dirbtinio intelekto technologijų reikia duomenų, kad jos galėtų efektyviau veikti. Gerai veikdamos jos gali padėti tobulinti ir automatizuoti sprendimų priėmimą toje pačioje srityje. Pavyzdžiui, dirbtinio intelekto sistema apmokoma ir tada naudojama kibernetiniams išpuoliams aptikti remiantis atitinkamo tinklo ar sistemos duomenimis. Panašiai kaip anksčiau garo variklis ar elektra, dirbtinis intelektas transformuoja mūsų pasaulį ir mūsų visuomenę[4].

Europos Sąjunga (ES) turėtų laikytis koordinuoto požiūrio, kad pasinaudotų visomis dirbtinio intelekto teikiamomis galimybėmis ir imtųsi naujų jo

[2] Гросс, Г. (2002). *Руководство для судебных следователей как система криминалистики*. XII.

[3] Jackson, C. (June 16, 2021). *Artificial Intelligence Changing the World of Forensics Science*: file:///D:/Downloads/EasyChair-Preprint-5815%20(1).pdf

[4] Dirbtinis intelektas yra Komisijos pramonės skaitmeninimo strategijos (COM(2016) 180 final) ir atnaujintos ES pramonės politikos strategijos (COM (2017) 479 final) dalis.

keliamų iššūkių. 2018 m. balandžio 10 d., 24 ES valstybės narės ir Norvegija įsipareigojo kartu siekti dirbtinio intelekto tikslų[5]. Bendrasis duomenų apsaugos reglamentas įsigaliojęs 2018 m. gegužės 25 d., tai yra svarbus žingsnis didinant pasitikėjimą, kuris ilgainiui taps būtinas tiek žmonėms, tiek įmonėms. Šiuo atžvilgiu ES tvarus požiūris į technologijas suteikia konkurencinį pranašumą, nes pokyčiai priimami laikantis Sąjungos vertybių[6]. Tam tikrais dirbtinio intelekto, kaip ir bet kurių kitų pokyčius lemiančių technologijų, atvejais gali kilti naujų etinio ir teisinio pobūdžio klausimų, pavyzdžiui, susijusių su atsakomybe arba galimai šališku sprendimų priėmimu. Todėl ES turi užtikrinti, kad dirbtinis intelektas būtų kuriamas ir diegiamas vadovaujantis tinkamu teisiniu pagrindu, kuriuo skatinamos naujovės laikantis Sąjungos vertybių ir pagrindinių teisių, taip pat etikos principų, pavyzdžiui, atskaitomybės ir skaidrumo. ES turi puikias galimybes vadovauti šioms diskusijoms pasauliniu lygmeniu.

Analizuojant dirbtinio intelekto sampratą, pažymėtina, kad tai yra ganėtinai naujas reiškinys, todėl vieningos nuomonės ir vieningai taikomo dirbtinio intelekto apibrėžimo šiuo metu neturime. Atsižvelgiant į tai, šiame straipsnyje bus aptariamos skirtingų mokslininkų t. y. S. J. Russel, P. Norvig, A. Turing, N. J. Nilsson nuostatos, kurios yra pripažįstamos kaip turinčios daugiausia įtakos kuriant teisinį reguliavimą, susijusį su dirbtiniu intelektu ir robotais.

Rašytiniuose šaltiniuose aptinkamos pirmosios įžvalgos, kuriose analizuojamas dirbtinis intelektas, parengtos 1943 m., darbo autoriais yra W. S. McCulloch ir W. H. Pitts[7]. Savo darbe jie rėmėsi trimis šaltiniais, t. y. a) psichologijos pagrindų ir neuronų funkcijų smegenyse žiniomis; b) S. J. Russell ir A. N. Whitehead teiginių logikos formalia analize bei, c) Turing skaičiavimo teorija[8]. Pirminį dirbtinį intelektą galima apibrėžti, kaip neuronų modelį, iš kurių kiekvienas neuronas gali būti apibūdintas, kaip „įjungtas“ arba „išjungtas“.

5 Austrija, Belgija, Bulgarija, Čekija, Danija, Estija, Suomija, Prancūzija, Vokietija, Vengrija, Airija, Italija, Latvija, Lietuva, Liuksemburgas, Malta, Nyderlandai, Lenkija, Portugalija, Slovakija, Slovėnija, Ispanija, Švedija ir Jungtinė Karalystė.

6 Europos Sąjungos sutarties 2 straipsnyje teigiama: „Sąjunga yra grindžiama šiomis vertybėmis: pagarba žmogaus orumui, laisve, demokratija, lygybe, teisine valstybe ir pagarba žmogaus teisėms, įskaitant mažumoms priklausančių asmenų teises.“Valstybės narės gyvena „visuomenėje, kurioje vyrauja pliuralizmas, nediskriminavimas, tolerancija, teisingumas, solidarumas, moterų ir vyrų lygybė.“

7 Mcculloch, W. S., Pitts, W. H. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics.* Vol. 5, 99–115: http://www.cs.cmu.edu/~./epxing/Class/10715/reading/McCulloch.and.Pitts.pdf

8 Mcculloch, W. S., Pitts, W. H. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics.* Vol. 5, 113: http://www.cs.cmu.edu/~./epxing/Class/10715/reading/McCulloch.and.Pitts.pdf

„Įjungtas“ jis yra tuo metu, kai atsako į stimuliaciją, paveiktą kitų neuronų[9]. Vienas iš svarbiausių dalykų, kuriuos pasiūlė mokslininkai, buvo idėja, kad dirbtinis intelektas gali mokytis[10], kurią vėliau išplėtojo kitas mokslininkas – D. O. Hebbas, o jo teorija yra žinoma ir taikoma ir šiuo metu.

Šiandien galima rasti įvairių dirbtinio intelekto apibrėžimų, tačiau prieš detaliau aptariant dirbtinio intelekto sąvoką, reikėtų išsiaiškinti, kas yra intelektas, ir kodėl ilgą laiką ši sąvoka buvo išskirtinai siejama tik su žmogui priklausančia savybe. Be jokios abejonės, intelektas, kaip ir dirbtinis intelektas, nuo tos dienos, kai jis buvo pradėtas tirti pirmą kartą, iki šių dienų yra daugelio skirtingų tyrimų objektas, todėl kiekvienas mokslininkas, apibrėždamas intelektą, remiasi skirtingomis teorijomis ir įgytomis žiniomis. Tai ir yra pagrindinė priežastis, kodėl vienintelės intelekto sąvokos nėra ir negali būti. Šiame straipsnyje intelektas bus apibrėžtas tiek, kiek yra būtina suprasti, kas yra dirbtinis intelektas.

Kalbant apie šiandienines galimybes naudotis didesniu duomenų kiekiu dirbtiniam intelektui sukurti reikia labai daug duomenų. Kompiuterio mokymas (dirbtinio intelekto rūšis) vyksta atliekant turimuose duomenyse esančių modelių atpažinimą ir taip įgytas žinias pritaikant naujiems duomenims[11]. Kuo didesnis duomenų rinkinys, tuo geresnes, net ir mažiau pastebimas, duomenų sąsajas galima nustatyti. Aplinka, kurioje sukaupta daug duomenų, suteikia daugiau galimybių ir tais atvejais, kai naudojamasi dirbtiniu intelektu. Taip yra todėl, kad algoritmas su savo aplinka susipažįsta ir su ja sąveikauja per duomenis. Pavyzdžiui, Fizinė valstybės sienos apsauga dažniausiai yra užtikrinama įvairiais būdais: vandenyse esančiais riboženkliais, kontrolinėmis pėdsakų juostomis, sausumos stulpeliais tiek miškingose vietovėse, tiek pievose, taip pat įvairaus pobūdžio užtvaromis[12]. Valstybė pastoviai stiprina fizinę sienų

9 Mcculloch, W. S., Pitts, W. H. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics.* Vol. 5, 113: http://www.cs.cmu.edu/~./epxing/Class/10715/reading/McCulloch.and.Pitts.pdf.

10 Mcculloch, W. S., Pitts, W. H. (1943). A logical calculus of the ideas immanent in nervous activity. *Bulletin of Mathematical Biophysics.* Vol. 5, 101: http://www.cs.cmu.edu/~./epxing/Class/10715/reading/McCulloch.and.Pitts.pdf.

11 Kai kuriais atvejais veiklos tikslas yra pats modelio atpažinimas: teksto ir duomenų gavyboje mokslininkai naudoja algoritmus dideliam tekstų (pvz. chemijos mokslinių darbų) skaičiui „perskaityti“ ir žinioms automatiškai surinkti (pvz. faktams, kurie nėra aiškiai nurodyti kuriame nors darbe, bet kuriuos galima rasti išanalizavus visą darbų rinkinį). Atnaujindama ES teisės aktus dėl autorių teisių Komisija nustatė išimtį teksto ir duomenų gavybai.

12 Lietuvos Respublikos Vyriausybės nutarimas „Dėl valstybės sienos ženklų, ženklinančių Lietuvos Respublikos sieną sausumoje ir pasienio vandenyse, formos, dydžio nustatymo ir jų statymo tvarkos aprašo patvirtinimo“. *Valstybės žinios,* 2007 m. kovo 21 d. Nr. 44–16: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.295850/asr

kontrolę, tačiau kontrolės metodai ir priemonės labai dažnai keičiasi tiek valstybės viduje, tiek už numatytos teritorijos ribų[13]. Valstybės sienų apsauga yra išplečiama už demarkuotų sienų ribų ir vykdoma naudojant daugybę nuotoliniu būdu valdomų sistemų, pavyzdžiui registracija prieš išvykimą iš valstybės, nuotolinis patikrinimas ir skaitmeninis stebėjimas atvykstančių, išvykstančių objektų. Toks stebėjimas gali užtikrinti tvarką, kad nebūtų pažeidžiami numatyti reikalavimai.

Tendencingumas ir diskriminacija yra bet kuriai visuomeninei ar ekonominei veiklai būdinga rizika. Žmogus, priimdamas sprendimus, nėra apsaugotas nuo klaidų ir neobjektyvumo. Tačiau DI neobjektyvumo padariniai galėtų būti kur kas didesni, dėl jo gali nukentėti ir būti diskriminuojami daug žmonių, nes nėra socialinės kontrolės mechanizmų, reguliuojančių žmonių elgesį[14]. Taip gali atsitikti ir tada, kai DI sistema vienu metu ir veikia, ir „mokosi". Tais atvejais, kai nepageidaujamų rezultatų negalima išvengti ar numatyti projektavimo etape, rizika kyla ne dėl pirminio sistemos projekto trūkumų, o dėl praktinio koreliacijų ar dėsningumų, kuriuos sistema nustato iš didelio duomenų rinkinio, poveikio.

Dėl daugeliui DI technologijų būdingų ypatybių, tokių kaip neskaidrumas (juodosios dėžės reiškinys), sudėtingumas, nenuspėjamumas ir dalinis autonomiškumas, gali būti sunku patikrinti jų atitiktį galiojančių ES teisės aktų, kuriais siekiama apsaugoti pagrindines teises, taisyklėms ir tai gali trukdyti veiksmingai užtikrinti jų vykdymą. Vykdymo užtikrinimo institucijoms ir poveikį patyrusiems asmenims gali trūkti priemonių patikrinti tai, kaip tam tikras sprendimas buvo priimtas naudojant DI, taigi ir tai, ar laikytasi atitinkamų taisyklių. Dėl tokių sprendimų nukentėjusiems fiziniams ir juridiniams asmenims gali kilti sunkumų veiksmingai pasinaudoti teise kreiptis į teismą.

Pavyzdžiui, kai kuriems DI algoritmams, naudojamiems nusikaltimų recidyvui prognozuoti, gali būti būdingas neobjektyvumas lyties ar rasės pagrindu, dėl kurio skirtingai nustatoma moterų ir vyrų arba piliečių ir užsieniečių

[13] Benedicto, A. R., Akkerman, M., Brunet, P. (2020). A Walled World: Towards a global apartheid. *Report, Transnational Institute*: https://www.tni.org/en/walledworld

[14] Komisijos Moterų ir vyrų lygių galimybių patariamasis komitetas šiuo metu rengia nuomonę dėl dirbtinio intelekto, kurioje, be kito poveikio, analizuojamas DI poveikis lyčių lygybei, ir planuoja ją priimti 2020 m pradžioje. DI ir lyčių lygybės ryšys taip pat nagrinėjamas 2020–2024 m. ES lyčių lygybės strategijoje 2020 m pradžioje Europos nacionalinių lygybės įstaigų tinklas (EQUINET) planuoja paskelbti (Robino Alleno ir DeeMasters) ataskaitą „Regulating AI: the new role for Equality Bodies – Meeting the new challenges to equality and non-discrimination from increased digitalisation and the use of AI".

recidyvo tikimybė[15]. Be to, sutinkame atvejų, "kai kurioms veido analizei skirtoms DI programoms būdingas neobjektyvumas lyties ar rasės pagrindu, dėl kurio analizuojant šviesesnės odos vyrų veidus daroma nedaug lyties nustatymo klaidų, tačiau daug jų daroma analizuojant tamsesnės odos moterų veidus"[16]. Pavyzdžiui, nuotolinis riziką keliančių žmonių atpažinimas, žvelgiant iš istorinės perspektyvos, atsirado visai neseniai, pradėjus pasienio tarnyboms taikyti įvairias technologijas, kurios veikia DI sistemų pagrindu. Ši asmenų, kertančių valstybės sieną, stebėjimo technologija skirta asmenims identifikuoti. Esminis šiuolaikinių valstybių sienų apsaugos poreikis yra identifikuoti asmenis, kurie atvyksta į valstybes[17]. DI technologijos taikymai yra pagristi tuo, kad atsiranda galimybė atlikti asmenų, kertančių valstybės sieną, kontrolę bei nustatyti galimus jų neteisėtus tikslus, užtikrinant saugumą nuo terorizmo bei kitų išpuolių atveju[18].

Vienas iš pagrindinių būsimos specialios DI reglamentavimo sistemos klausimų – nustatyti jos taikymo aprėptį. Daroma pradinė prielaida, kad reglamentavimo sistema būtų taikoma DI produktams ir paslaugoms. Todėl šioje baltojoje knygoje ir visose būsimose politikos iniciatyvose dirbtinis intelektas turėtų būti aiškiai apibrėžtas. Pirmąją DI apibrėžtį Komisija pateikė komunikate „Dirbtinis intelektas Europai[19]- „Dirbtinis intelektas – tai sistemos, kurios elgiasi protingai, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti. Dirbtinio intelekto sistemos gali būti grindžiamos vien tik programine įranga ir veikti virtualiajame pasaulyje (pvz., balso sintezatoriai, vaizdo analizės programinė įranga, paieškos sistemos, kalbos ir veido atpažinimo sistemos) arba gali būti integruotos techninėje įrangoje (pvz., pažangiuose robotuose, savivaldžiuose automobiliuose, bepiločiuose orlaiviuose ar daiktų interneto objektuose)". Šią apibrėžtį patikslino Aukšto lygio ekspertų

15 Tolan, S., Miron, M., Gomez, E., Castillo, C. (2019). Why Machine Learning May Lead to Unfairness: Evidence from Risk Assessment for Juvenile Justice in Catalonia. *Materials of International Conference on AI and Law.*

16 Buolamwini, J., Gebru, T. (2018). Proceedings of the 1st Conference on Fairness, Accountability and Transparency. *PMLR*, 81. 77–91.

17 Scot, J. C. (2008). *How certain schemes to improve the human condition have failed*: https://politicalscience.yale.edu/publications/seeing-state-how-certain-schemes-improve-human-condition-have-failed

18 Shachar, A. (2020). Borders in the Time of COVID-19. *Ethics and International Affairs:* https://www.ethicsandinternationalaffairs.org/2020/borders-in-the-time-of-covid-19/

19 Europos Komisijos Komunikatas Europos Parlamentui, Europos Vadovų tarybai, Tarybai, Europos Ekonomikosir Socialinių reikalų komitetui ir regionu komitetui. *Dirbtinis intelektas Europai* {SWD(2018) 137 final}, 2018 04 25 COM(2018) 237 final. 1.

grupė[20], pateikdama suformuluotą DI apibrėžtį – „Dirbtinio intelekto (DI) sistemos yra žmonių sukurtos programinės įrangos (taip pat gali būti aparatinės įrangos) sistemos, kurios, joms nustačius sudėtingą tikslą, veikia fiziniu ir skaitmeniniu lygmenimis – įvertina savo aplinką rinkdamos duomenis, aiškina surinktus struktūruotus ir nestruktūruotus duomenis, logiškai analizuoja turimas žinias arba apdoroja pagal tuos duomenis suformuotą informaciją ir priima sprendimą, kokį (-ius) veiksmą (-us) geriausia atlikti, kad užsibrėžtas tikslas būtų pasiektas. DI sistemos gali naudoti simbolines taisykles arba išmoktą skaitmeninį modelį, jos taip pat gali koreguoti savo elgesį analizuodamos, kokį poveikį aplinkai padarė jų ankstesni veiksmai“. Taigi, kuriame naujame teisiniame dokumente DI apibrėžtis turės būti pakankamai lanksti, kad būtų galima atsižvelgti į technikos pažangą, ir kartu pakankamai tiksli, kad būtų užtikrintas būtinas teisinis tikrumas. Gali būti ir išimtinių atvejų, kai dėl keliamo pavojaus tam tikroms reikmėms naudojamos DI prie taikos savaime laikytinos labai rizikingomis, tai yra nepriklausomai nuo konkretaus sektoriaus, ir joms toliau aptariami reikalavimai vis tiek būtų taikomi[21]. DI gali labai padėti siekti ES saugumo strategijos tikslų. Jis gali būti strateginė priemonė, suteikianti galimybę kovoti su esamomis grėsmėmis ir numatyti tiek būsimą riziką, įskaitant hibridines grėsmes, tiek galimybes. DI gali padėti kovoti su nusikalstamumu ir terorizmu ir sudaryti teisėsaugos institucijoms sąlygas sekti sparčią nusikaltėlių naudojamų technologijų raidą ir jų tarpvalstybinę veiklą[22]. Kita vertus, DI naudojimas kelia ir įvairią mažintiną riziką. Veido atpažinimo sistemų naudojimas viešosiose erdvėse gali labai pakenkti privatumui, nebent būtų tinkamai reglamentuojamas. Be to, netinkamai išmokytos ir suprojektuotos DI sistemos gali padaryti didelių klaidų, galinčių pažeisti privatumo ir nediskriminavimo principus[23]. DI grindžiami robotai ir intelektinės sistemos turi būti kuriami ir projektuojami taip, kad atitiktų tokius pat aukštus saugos ir pagrindinių teisių

20 Europos Komisija „Europos Komisijos Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais sukurtoje DI apibrėžtyje“ 2018 m. gruodžio 7 d., 795 galutinis: https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04–11e8-a96d-01aa75ed71a1.0011.02/DOC_2&format=PDF

21 Pažymėtina, kad gali būti taikomi ir kiti ES teisės aktai. Pavyzdžiui, DI prie taikų, integruojamų į vartojimo prekes, saugai gali būti taikoma Direktyva dėl bendros gaminių saugos.

22 Komisijos Komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir Socialinių reikalų Komitetui ir Regionų Komitetui Europos požiūrio į dirbtinį intelektą formavimas: https://www.infolex.lt/teise/default.aspx?id=1929&crd=1245300

23 2020 m. kovo mėn. ES lyčių lygybės strategiją (COM(2020)152), 2020m. rugsėjo mėn. ES kovos su rasizmu veiksmų planą (COM(2020)565), 2020m. lapkričio mėn. ES LGBTIQ asmenų lygybės strategiją (COM(2020)698) ir 2021m. kovo mėn. Neįgaliųjų teisių strategiją (COM(2021)101).

apsaugos standartus, kokius pagal Europos teisės aktus turi atitikti tradicinės technologijos. Galima paminėti atvejį, kai: DI prie taikos, naudojamos nuotoliniam biometriniam tapatybės nustatymui[24], <...> „Nuotolinį biometrinį tapatybės nustatymą reikėtų skirti nuo biometrinio sutikrinimo (pastarasis yra saugumo procedūra, kurią taikant pagal asmens unikalias biologines ypatybes patikrinama, ar asmuo yra tas, kuo teigia esąs). Nuotolinis biometrinis tapatybės nustatymas – nuotoliniu būdu viešoje erdvėje nenutrūkstamai vykdomas daugelio asmenų tapatybės nustatymas pagal biometrinius identifikatorius (pirštų atspaudus, veido atvaizdą, rainelę, kraujagyslių raštą ir kt.) lyginant juos su duomenų bazių duomenimis“ <...>, ir kitoms intervencinėms sekimo technologijoms, visada būtų laikomos labai rizikingomis, todėl joms visada būtų taikomi toliau aptariami reikalavimai.

Išskiriami specialūs nuotolinio biometrinio tapatybės nustatymo reikalavimai – renkant ir naudojant biometrinius duomenis[25], tapatybei nustatyti nuotoliniu būdu[26], – taikant veido atpažinimo technologijas, tapatybė nustatoma asmens veido atvaizdo šabloną lyginant su daug kitų duomenų bazėje saugomų šablonų, siekiant sužinoti, ar joje saugomas tas atvaizdas. Atliekant biometrinį sutikrinimą, priešingai, atvaizdas palyginamas su vienu atvaizdu. Jis leidžia palyginti du biometrinius šablonus, paprastai darant prielaidą, kad jie priklauso tam pačiam asmeniui. Lyginami du biometriniai šablonai siekiant nustatyti, ar abu atvaizdai yra to paties asmens. Tokia procedūra įdiegta, pavyzdžiui, automatizuotos sienų kontrolės vartuose, kurie naudojami oro uostuose patikrinimams kertant sieną atlikti. Pavyzdžiui, diegiant veido atpažinimo technologijas viešose vietose, kyla tam tikra pagrindinių teisių pažeidimo rizika[27]. Nuotolinio biometrinio tapatybės nustatymo DI sistemų naudojimo poveikis

24 2020 m. vasario mėn. Europos Komisijos baltoji knyga dėl dirbtinio intelekto (COM(2020)65).

25 Biometriniai duomenys yra „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 [pirštų atspaudų] duomenys“. Teisėsaugos direktyvos 3 straipsnio 13 punktas, BDAR 4 straipsnio 14 punktas, Reglamento (ES) 2018/1725 3 straipsnio 18 punktas.

26 Biometriniai duomenys yra „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 [pirštų atspaudų] duomenys“. Teisėsaugos direktyvos 3 straipsnio 13 punktas, BDAR 4 straipsnio 14 punktas, Reglamento (ES) 2018/1725 3 straipsnio 18 punktas.

27 Pavyzdžiui, žmogaus teisės į orumą. Didžiausią susirūpinimą, susijusį su pagrindinėmis teisėmis, naudojant veido atpažinimo technologijas kelia teisės į privatų gyvenimą ir asmens duomenų apsaugą pažeidimai. Taip pat gali būti daromas poveikis tam tikrų grupių, pavyzdžiui, vaikų, vyresnio amžiaus asmenų ir neįgaliųjų, nediskriminavimui ir teisėms. Naudojant šią technologiją neturi būti pažeidžiama ir teisė į saviraiškos, asociacijų ir susirinkimų laisvę. Žr.

pagrindinėms teisėms gali labai skirtis priklausomai nuo jų naudojimo tikslo, aplinkybių ir masto.

ES duomenų apsaugos taisyklėmis iš esmės draudžiama tvarkyti biometrinius duomenis siekiant konkrečiai nustatyti fizinio asmens tapatybę, išskyrus atvejus, kai tenkinamos specialios sąlygos[28]. Pagal Bendrąjį duomenų apsaugos reglamentą toks duomenų tvarkymas gali būti atliekamas tik dėl kelių priežasčių, o pagrindinė iš jų – svarbus viešasis interesas. Tokiu atveju duomenys turi būti tvarkomi pagal ES arba nacionalinę teisę, laikantis proporcingumo reikalavimų, nepažeidžiant esminių teisės į duomenų apsaugą nuostatų ir užtikrinant tinkamas apsaugos priemones. Pagal Teisėsaugos direktyvą toks duomenų tvarkymas turi būti tikrai būtinas, iš esmės leidžiamas pagal ES arba nacionalinę teisę ir atliekamas taikant tinkamas apsaugos priemones. Kadangi bet koks biometrinių duomenų tvarkymas siekiant konkrečiai nustatyti fizinio asmens tapatybę yra ES teisėje nustatyto draudimo išimtis, jam būtų taikoma ES pagrindinių teisių chartija.

Kaip jau buvo minėta anksčiau, vienintelės nuomonės, kas yra dirbtinis intelektas, nėra, tačiau daugelis mokslininkų yra pritarę N. J. Nilsson išskirtai dirbtinio intelekto sąvokai, kad tai yra tokia veikla, kuri yra skirta protingų mašinų gamybai, o intelektas – tai kokybė, leidžianti subjektui tinkamai veikti savo aplinkoje[29].

Paminėtina, kad šiuo metu nėra jokio įsigaliojusio teisės akto, reglamentuojančio dirbtinio intelekto apibrėžimą ar veiklos ribas, tačiau yra svarstomas 2017 m. sausio 27 d. Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų[30] (toliau – „Pranešimas“). Viena iš šio Pranešimo parengimo priežasčių yra ta, kad „žmonija stovi ant naujos eros slenksčio, kai dar labiau patobulinti robotai, botai, androidai ir kitos dirbtinio intelekto išraiškos gali sukelti naują pramonės revoliuciją, galinčią persmelkti visą visuomenę, todėl itin svarbu teisės aktų leidėjams apsvarstyti visas šio reiškinio teisines ir etines pasekmes bei poveikį, netrukdant

Facial recognition technology: fundamental rights considerations in the context of law enforcement: https://fra.europa.eu/en/publication/2019/facial-recognition.

28 BDAR 9 straipsnis, Teisėsaugos direktyvos 10 straipsnis. Taip pat žr. Reglamento (ES) 2018/1725 (taikomo ES institucijoms ir įstaigoms) 10 straipsnį. Bendrasis duomenų apsaugos reglamentas toliau tekste – (BDAR).

29 Nilsson, N. J. (2010). *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. 77.

30 2017 m. sausio 27 d. Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)).

diegti inovacijų“[31]. Ši mokslo sritis be jokios abejonės gali būti laikoma pačia naujausia akademine, bet ne praktine sritimi. Pagrindiniais šios mokslo srities vystytojais gali būti laikomi universitetai, įtraukę dirbtinio intelekto programas į savo studijas.

Taigi, išanalizavus šiuo metu egzistuojančias dirbtinio intelekto sąvokas, galima daryti pagrįstą išvadą, kad dirbtinis intelektas ir intelektas yra glaudžiai tarpusavyje susiję reiškiniai, kadangi dirbtinio intelekto veikimas remiasi žmogaus intelekto principais. Taip pat paminėtina, kad dirbtinio intelekto pagrindiniai požymiai yra gebėjimas mąstyti, suvokti, spręsti problemas, mokytis ir kt. Vienintelis skirtumas tarp dirbtinio intelekto nuo žmogaus intelekto – tai prigimtis, kadangi dirbtinis intelektas yra dirbtinai sukurtas žmogaus. Kaip pažymi, prof. Valery Shepitko[32], novatoriška teisėsaugos sritis yra algoritmų (kūrimas) nustatymas. Informacinių technologijų diegimas, jų panaudojimas nusikaltimų tyrime ženkliai padidintų tyrėjų (prokurorų ir kt.) produktyvumą tiriant organizuoto nusikalstamumo nusikaltimus. Tokios technologijos padeda tyrėjui sisteminti pagal laiką, rūšis, organizuotos nusikalstamos grupuotės tikslus, motyvus ir kt., Be to, pažymėtina, kad <...> „nusikaltėliams naudojant naujausius mokslo ir technikos pasiekimus, tyrėjas irgi turi keisti savo darbo stilių“[33]. Apibendrinant pažymėtina, kad DI yra viena iš kriminalistikos mokslo plėtros sričių. Kaip pavyzdį galima paminėti, kad asmenų identifikavimo problemos tapo ypač aktualios pastaruoju laikotarpiu nelegalios migracijos srityje, kai asmenys masiškai pradėjo kirsti valstybių sienas, naudodami suklastotus ar negaliojančius dokumentus[34]. Valstybės sienos apsaugos sistemoje taikoma vis naujų DI technologijų, tai yra skatinama ES lygmenyje, ypač daug dėmesio skiriant saugaus DI sistemų naudojimo užtikrinimui[35].

Pagrindinės teisės į asmens duomenų apsaugą

Pagrindinis nagrinėjimo aspektas – asmenų duomenų apsauga nuo dirbtinio intelekto. Analizuojant šį klausimą bus aptartos teisės bei laisvės, kurios labiausiai gali būti pažeistos dėl dirbtinio intelekto veiksmų ar neveikimo. Taip

31 2017 m. sausio 27 d. Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)).

32 Shepitko, V. *Introduction to Criminalistics*. 60.

33 Берназ, И. Д. (2012). Стратегическое планирование при расследовании преступлений. Современное состояние и развитие криминалистики. 24.

34 Todorov, A. (2017). *Face value: the irresistible influence of first impressions*: https://press.princeton.edu/books/hardcover/9780691167497/face-value

35 Crowford, K. (2021). Time to regulate AI that interprets human emotions. *Nature*: https://www.nature.com/articles/d41586–021–00868–5

pat bus ieškoma sprendimo būdų, kaip būtų galima patobulinti esamą reguliavimą bei bus bandoma išsiaiškinti, kokio reguliavimo šiuo metu trūksta.

DI naudojimas gali daryti poveikį pamatinėms ES vertybėms ir pažeisti pagrindines teises[36], įskaitant teisę į saviraiškos laisvę, susirinkimų laisvę, žmogaus orumą, nediskriminavimą dėl lyties, rasinės arba etninės kilmės, religijos ar tikėjimo, negalios, amžiaus arba seksualinės orientacijos, kai tai aktualu tam tikrose srityse, teisę į asmens duomenų ir privatumo apsaugą[37]arba teisę į veiksmingą teisminę gynybą ir teisingą bylos nagrinėjimą, taip pat neatitikti vartotojų apsaugos taisyklių. Ši rizika gali kilti dėl to, kad yra bendrųjų DI sistemų projektavimo trūkumų (be kita ko, susijusių su žmogaus atliekama priežiūra), arba dėl to, kad naudojami neobjektyvūs duomenys (pvz., sistemai mokyti naudojami tik, arba daugiausia, vyrų duomenys, todėl moterų atžvilgiu gaunami neoptimalūs rezultatai).

DI gali atlikti daug funkcijų, kurias anksčiau galėjo atlikti tik žmogus. Todėl fiziniai ir juridiniai asmenys vis dažniau susidurs su veiksmais ir sprendimais, kurie bus priimami DI sistemų arba jomis naudojantis ir kuriuos kartais gali būti sunku suprasti ir prireikus veiksmingai užginčyti. Be to, DI suteikia daugiau galimybių stebėti ir analizuoti kasdienius žmonių įpročius. Pavyzdžiui, esama rizikos, kad valstybės institucijos ar kiti subjektai, pažeisdami ES duomenų apsaugos ir kitas taisykles, gali naudoti DI masinio sekimo tikslais, o darbdaviai – stebėti, kaip elgiasi jų darbuotojai. Analizuojant didelius duomenų kiekius ir nustatant jų sąsajas, DI taip pat gali būti naudojamas asmens duomenims atsekti ir išanoniminti, taip iškiltų naujo pobūdžio pavojus asmens duomenų apsaugai net ir tada, kai pačiuose duomenų rinkiniuose asmens duomenų nėra. Interneto tarpininkai taip pat naudoja DI siekdami nustatyti naudotojus dominančios informacijos prioritetus ir parinkti jiems turinį. Tai, kaip tvarkomi duomenys, projektuojamos prietaikos ir kokią galimybę įsikišti turi žmogus, gali turėti įtakos teisėms į saviraiškos laisvę, asmens duomenų apsaugą bei privatumą ir politinėms laisvėms.

Pirmiausia, analizuojant aukščiau paminėtus klausimus, reikėtų atkreipti dėmesį į Europos Sąjungos požiūrį į tam tikrų sričių reguliavimo sukūrimą. Šumano deklaracijoje yra nurodyta, kad „Europos negalima sukurti vienu mostu arba pagal vienintelį planą. Ji bus sukurta pasiekus konkrečių laimėjimų, kurie

36 Europos Tarybos tyrimai rodo, kad DI gali daryti poveikį daugeliui pagrindinių teisių: https://rm.coe.int/algorithms-andhuman-rights-en-rev/16807956b5.

37 Šiai rizikai mažinti priimtas Bendrasis duomenų apsaugos reglamentas (BDAR) ir E. privatumo direktyva (deramasi dėl naujo e. privatumo reglamento), tačiau gali reikėti išnagrinėti, ar DI sistemos nekelia daugiau rizikos. Komisija nuolat stebės BDAR taikymą ir jį vertins.

pirmiausia sudarys sąlygas atsirasti tikram solidarumui“[38]. Todėl Europos Sąjungoje laikomasi pozicijos, kad priimant bet kokias iniciatyvas, šiuo atveju robotikos ir dirbtinio intelekto srityje, reikėtų atsižvelgti į laipsnišką, pragmatišką ir atsargų požiūrį[39].

Prieš išsamesnį teisių ir laisvių aptarimą apsaugos nuo dirbtinio intelekto kontekste, būtina paminėti ir I. Asimovo dėsnius[40]: a) robotui nevalia sužeisti žmogaus ar per savo neveiklumą leisti žmogui patirti skriaudą; b) robotas turi klausyti žmogaus jam duotų nurodymų, nebent jie prieštarautų pirmajam dėsniui; c) robotas turi saugoti savo paties egzistavimą, nebent toks saugojimas prieštarautų pirmajam ir antrajam dėsniui. Šiuos dėsnius „reikia traktuoti kaip taikytinus robotų, įskaitant robotus, turinčius integruotą autonominio veikimo ir savarankiško mokymosi režimą, kūrėjams, gamintojams ir operatoriams, kadangi šių dėsnių negalima paversti mašininiu kodu“[41]. Taigi toliau šiame straipsnyje bus aptartos asmenų teisės bei laisvės apsaugos nuo dirbtinio intelekto kontekste.

Pradžioje, atkreipiamas dėmesys į *asmens teisę į duomenų apsaugą,* kadangi šiuo metu pagrindinis interneto verslo modelis yra glaudžiai susijęs su didelio masto stebėjimu, kas kelia grėsmę žmonijai[42]. Ryškiausias pastarųjų metų pavyzdys yra *Facebook* socialinis tinklas, kuris stebi žmonių veiklą pasitelkiant internetą, netgi jeigu jie nėra *Facebook* nariai (vartotojai) bei tikėtina, kad pasidalino su trečiosiomis šalimis savo vartotojų (~ 87 mln.) duomenimis be jų žinios ir sutikimo, tokių būdu pažeidžiant vartotojų teisę į duomenų apsaugą[43]. Toks stebėjimas gali atskleisti pačią jautriausią informaciją apie asmenis, t. y. nuo tokių paprasčiausių duomenų, kaip vardas, pavardė, elektroninis paštas, telefono numeris ir kt. iki informacijos apie asmens tautybę, rasę, seksualinę orientaciją, politines pažiūras, socialinę padėtį, sveikatą, biometrinius duomenis ir t. t. Analizuojant asmens teisę į duomenų apsaugą, paminėtini toliau nagrinėjami teisės aktai, t. y. Konvencija dėl asmenų apsaugos ryšium su asmens

38 1950 m. gegužės 9 d. Šumano deklaracija: https://europa.eu/european-union/about-eu/symbols/europe-day/schuman-declaration_lt.

39 2017 m. sausio 27 d. Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)), 6.

40 Asimov, I. (1943). *I, Robot.*

41 2017 m. sausio 27 d. Europos Parlamento pranešimas su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)), 6.

42 Schneier, B. (2013). *The Public-Private Suveillance Partnership*: https://www.bloomberg.com/view/articles/2013–07–31/the-public-private-surveillance-partnership

43 Schneier, B. (2013). *The Public-Private Suveillance Partnership*: https://www.bloomberg.com/view/articles/2013–07–31/the-public-private-surveillance-partnership

duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis[44] (toliau – „Konvencija Nr. 108“), ir Lietuvos Respublikos įstatymas dėl Protokolo[45], Europos Sąjungos pagrindinių teisių chartija, Sutartis dėl Europos Sąjungos veikimo (toliau – „SESV“), 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)[46] (toliau – „BDAR“).

Galima teigti, kad šiuo metu didžiausias dėmesys yra atkreipiamas būtent į BDAR, kadangi šiuo reglamentu yra nustatoma asmens duomenų apsaugos teisinė sistema pasitelkiant netgi automatizuotas priemones. BDAR 4 straipsnyje yra įtvirtinta, kad „duomenų tvarkymas – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant, platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimais, ištrynimas arba sunaikinimas“[47].Taigi, BDAR sudaro galimybę tvarkyti asmenų duomenis dviem būdais, tačiau būtent automatizuotas duomenų tvarkymas yra šio darbo nagrinėjimo dalykas, kadangi tai gali būti dirbtinio intelekto sukurta programinė įranga (įranga, sukurta pasitelkiant dirbtinį intelektą), kuri gali sukelti neigiamas pasekmes dėl netinkamo ar neleistino duomenų tvarkymo. BDAR 22 straipsnio 1 dalyje yra įtvirtinta duomenų subjekto teisė, „kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam

44 Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis. *Valstybės žinios,* 2001, Nr. 32–1055.

45 Lietuvos Respublikos įstatymas dėl Protokolo, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, ratifikavimo (TAR, 2019–11–13, Nr. 2019–18188) Įstatymas dėl Protokolo, kuriuo iš dalies keičiama Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, ratifikavimo: https://www.infolex.lt/ta/558614

46 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, 1–88.

47 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, 1–88.

kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį“[48]. Toks reglamentavimas leidžia daryti išvadą, kad duomenų subjektui negali būti apribota galimybė rinktis dėl jo duomenų tvarkymo būdo (formos). Šis BDAR sureguliuotas klausimas yra itin aktualus, kadangi interneto plėtra kelia problemų dėl duomenų tvarkymo skaidrumo ir asmenims dažnai kyla klausimas, kokiu būdu galima užtikrinti savo teisių apsaugą, kad nebūtų tvarkomi pertekliniai asmenų duomenys. DI taip pat gali pagerinti kibernetinį saugumą, pavyzdžiui, padėdamas rinkti žvalgybos informaciją apie grėsmes– pagal ankstesnę patirtį atpažindamas tendencijas, sumažindamas reagavimo į incidentus laiką ir sudarydamas geresnes sąlygas laikytis geriausios saugumo praktikos[49]. Taip pat galima paminėti, kad 2021 m. balandžio 14d. Komisija taip pat pristatė naują ES kovos su organizuotu nusikalstamumu strategiją, kuria siekiama užtikrinti modernų atsaką į technologines tendencijas, įskaitant DI naudojimą nusikalstamos veikos tyrimuose, pvz., didelių duomenų kiekių analizei arba tamsiojo interneto tyrimams[50]. Taigi pastebėtina ir tai, kad nuskenuoti asmenų veidą, jų išraišką bei emocijas, tokiu būdu pažeidžiant asmenų duomenų apsaugą (biometrinius duomenų). Pastaroji duomenų rūšis laikoma ypatingos svarbos duomenimis, kadangi tai yra itin individualu ir žmogus net gali nesuprasti, kad yra kaupiami tokio pobūdžio jo duomenys ir galimai panaudojami tam tikrais neteisėtais tikslais. Didžiausios technologijų kompanijos, t. y. *Google, Apple, Microsoft, Facebook* ir *Amazon* jau šiuo metu tvarko asmenų duomenis tiek tam tikrąją dalį jų sutikimu, tiek ir kitus duomenis, kuriems savo sutikimo asmenys (vartotojai) nėra davę. Tačiau šiuo atveju itin sunku įrodyti tokių duomenų tvarkymo procesą.

Kita svarbi paminėtina *teisė į teisingą teismą*. Atkreiptinas dėmesys, kad ši teisė yra įtvirtinta EŽTK 6 straipsnyje[51]. Šiuo metu teismai vis daugiau bando automatizuoti savo veiklą, t. y. naudotis automatizuotomis sistemomis ir kitais robotais su programine įranga, kuri galėtų smarkiai sumažinti teismo

48 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, 1–88.

49 Komisijos Komunikatas Europos Parlamentui, Tarybai, Europos Ekonomikos ir Socialinių reikalų komitetui ir regionų Komitetui Europos požiūrio į dirbtinį intelektą formavimas: https://www.infolex.lt/teise/default.aspx?id=1929&crd=1245300#footnote229

50 Europos Komisijos komunikatas dėl 2021–2025 m. ES kovos su organizuotu nusikalstamumu strategijos (COM(2021)170 final.

51 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995, Nr. 40–987.

proceso trukmę ir netgi priimti nuoseklesnius teisinius sprendimus negu tai galėtų padaryti žmonės. Dirbtinis intelektas, o būtent jo pagalba sukurti algoritmai, gali padėti įvertinti bylą ir netgi apskaičiuoti bylos laimėjimo galimybių tikimybę. Dirbtinio intelekto naudojimas gali ne tik lemti bylų sumažėjimą, bet toks programinės įrangos naudojimas gali padėti teisėjams užtikrinti teisę į teisingą teismą[52]. Nors ir dirbtinio intelekto nauda šioje srityje yra akivaizdi, tačiau reikia priminti du principus, į kuriuos turi būti atsižvelgta, kai teisėjai naudosis autonominėmis priemonėmis kaip pagalbininkais priimant sprendimus, t. y. atskaitomybės išlaikomumas ir atpažįstamumas[53]. Šie principai yra itin svarbūs kadangi teisėjai turi suprasti, kokiu būdu veikia atitinkamas dirbtinis intelektas, kaip tai gali daryti įtakos jų priimamiems sprendimas; teisėjas turi būti atsakingas už priimtą galutinį sprendimą, nepriklausomai nuo to, ar sprendimas priimtas su ar tik pagalbinės sistemos (kompiuterio) pagalba; teisėjo nukrypimas nuo pagalbinės sistemos (kompiuterio) varianto turi būti atitinkamai užfiksuotas[54]. Taip pat egzistuoja nuomonė, kad dirbtinis intelektas gali veikti pažeidžiant nešališkumo principą[55]. Toks atvejis buvo užfiksuotas tuomet, kai programinė įranga, kuri naudojama siekiant nustatyti užstatą buvo priešiškai nusiteikusi prieš afroamerikiečius, tokios programinės įrangos nauda nebuvo aiški[56]. Taigi, darytina išvada, kad nors gali atrodyti, kad klausimai, susiję su dirbtinio intelekto naudojimu užtikrinant asmenų teisę į teisingą teismą negali pakenkti asmenims, tačiau tai gali būti klaidinga. Svarbiausia užtikrinant asmenų teises į teisingą teismą, tuomet kai sprendimų priėmimo procese dalyvauja dirbtinis intelektas, yra teisėjų ir kitų byloje dalyvaujančių byloje asmenų galimybė patikrinti kokiu būdu dirbtinis intelektas priėjo prie vienokios ar kitokios išvados. Dirbtinis intelektas yra ypatingai naudingas įgyvendinant

52 Technological convergence, artificial intelligence and human rights. (2017). *Parliamentary Assembly.* 11–12: http://website-pace.net/documents/19871/3306947/20170322-artificial+intelligence-humanrights-EN.pdf/d4e33dee-e37e-4537–96a8-f207c3903081

53 Technological convergence, artificial intelligence and human rights. (2017). *Parliamentary Assembly.* 12: http://website-pace.net/documents/19871/3306947/20170322-artificial+intelligence-humanrights-EN.pdf/d4e33dee-e37e-4537–96a8-f207c3903081

54 Technological convergence, artificial intelligence and human rights. (2017). *Parliamentary Assembly.* 12: http://website-pace.net/documents/19871/3306947/20170322-artificial+intelligence-humanrights-EN.pdf/d4e33dee-e37e-4537–96a8-f207c3903081

55 Smith, M. (2016) In Wisconsin, a Backlash Against Using Data to Foretell Defendants' Futures. *The New York Times*: https://www.nytimes.com/2016/06/23/us/backlash-in-wisconsin-against-using-data-to-foretell-defendants-futures.html

56 Corbett-Davies, S., Pierson E., Feller. A. *et. al.* A Computer program used for bail and sentencing decisions was labeled biased against blacks. It'sactually not that clear. (2016). *The Washington Post*: https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas/?utm_term=.18934fd93df9.

šią asmenų teisę nesudėtingose bylose eliminuojant žmogiškos klaidos faktorių, tačiau galutinis sprendimas turi būti patikrintas teisėjo bei jo patvirtintas. Taigi, pritartina tokio dirbtinio intelekto panaudojimui, tačiau siūloma neeliminuoti žmogiškojo faktoriaus, t. y. būtina, kad „tikrasis" teisėjas patikrintų ir patvirtintų dirbtinio intelekto priimtą sprendimą.

Apibendrinant visa tai, kas buvo paminėta, įvertinus tarptautinius ir Europos Sąjungos teisės aktus, reguliuojančius pagrindines žmogaus teises ir laisves, manytina, kad ypatingą dėmesį reikia skirti tokių teisių ir laisvių apsaugai, kaip asmens teisė į duomenų apsaugą, privatų ir šeimos gyvenimą, orumą, saugą, saugumą, nuosavybės teisę, laisvę reikšti mintis ir įsitikinimus bei diskriminacijos uždraudimą. Šios teisės ir laisvės gali būti laikomos patenkančiomis į didžiausią jų pažeidimo riziką dėl dirbtinio intelekto naudojimo sukuriamo poveikio. Todėl priimant teisės aktus dirbtinio intelekto reguliavimo srityje reikėtų nurodyti šias asmenų teises ir laisves bei atitinkamai nustatyti jų saugojimo kriterijus. Vienas iš tokių Europos Sąjungos tikslų leidžia daryti išvadą, kad Europos Sąjunga atsižvelgia į skaitmeninės eros spartų pasikeitimą, todėl ir atitinkamas reguliavimas padėtų išvengti Europos Sąjungos bendruomenės teisių ir laisvių pažeidimų. Tuo pačiu siūloma atsižvelgti į jau egzistuojantį teisinį pagrindą asmenų teisių ir laisvių apsaugos srityje, kadangi ne visada naujų teisės aktų priėmimas gali būti toks veiksmingas, kaip jau esamų patobulinimas.

Išvados

Pažymėtina, kad ir praėjus šimtmečiui Hanso Grosso mintys šiuolaikiniu kriminalistikos reformos laikotarpiu neprarado savo reikšmės tiriant nusikalstamas veikas. Dar H. Grossas, apibendrinęs sukauptą nusikaltimo tyrimo praktiką ir reikšmingiausius mokslo atradimus bei savo tyrinėjimus, juos susisteminęs į savarankišką mokslo žinių šakai būdingą visumą, tuo visą susikaupusią, tačiau išsibarsčiusią ir gana chaotišką kriminalistikai vertingą informaciją pavertė darnia kriminalistinių mokslinių žinių sistema ir pavartojo patį terminą „kriminalistika", taip apibūdindamas mokslą apie baudžiamosios teisės realijas. H. Grosas rašė: „kriminalistika pagal savo prigimtį prasideda ten, kur baudžiamoji teisė, irgi pagal savo prigimtį, baigia darbą: materialinės baudžiamosios teisės dalykas yra nusikalstamos veikos ir bausmės tyrimas, formali baudžiamoji teisė (procesas) apima materialinės baudžiamosios teisės taikymo taisykles. Tačiau kokiu būtent būdu vykdomi nusikaltimai? Kaip ištirti šiuos būdus ir juos išaiškinti, kokie buvo to padarymo motyvai, kokie tikslai – apie tai mums nekalba nei baudžiamoji teisė, nei procesas. Tai sudaro kriminalistikos

dalyką“[57].

DI – strateginė technologija, kuri yra labai naudinga piliečiams, įmonėms ir visai visuomenei, jeigu ji yra orientuota į žmogų, etiška, tvari ir paiso pagrindinių teisių ir vertybių. DI labai padidina veiksmingumą ir našumą, o tai savo ruožtu gali padidinti Europos pramonės konkurencingumą ir piliečių gerovę. Jis taip pat gali padėti spręsti kai kurias opiausias visuomenės problemas, taip pat padėti kovoti su klimato kaita ir aplinkos būklės blogėjimu, spręsti tvarumo ir demografijos problemas, apsaugoti mūsų demokratiją ir, kai būtina ir proporcinga, kovoti su nusikalstamumu.

Kad Europa galėtų visapusiškai pasinaudoti DI teikiamomis galimybėmis, reikia plėtoti ir stiprinti reikiamus pramoninius ir technologinius pajėgumus. Kaip nurodyta kartu skelbiamoje Europos duomenų strategijoje, tam taip pat reikia priemonių, kurios sudarytų sąlygas ES tapti pasauliniu duomenų centru. Formuojant Europos požiūrį į DI siekiama skatinti Europos pajėgumą kurti DI inovacijas ir kartu remti etiško ir patikimo DI plėtotę ir diegimą visoje ES ekonomikoje. DI turėtų būti naudingas žmonėms ir užtikrinti visuomenės gerovę.

Siekiant sureguliuoti dirbtinį intelektą, svarbu prieiti prie vieningo dirbtinio intelekto apibrėžimo. Nors mokslininkai yra išskyrę daugelį dirbtinio intelekto sampratų, tačiau bendrai galima teigti, kad dirbtinis intelektas – tai sistema, susijusi su sparčiai besivystančiomis technologijomis, kurios gali veikti intelektualiai, t. y. kaip žmogus. Dauguma autorių taip pat pritaria, kad dirbtinio intelekto mokslo tikslas yra sukurti protingus dirbtinius darinius, galinčius savarankiškai mąstyti, mokytis, spręsti problemas ir kt. Tokio apibrėžimo naudojimas leistų lengviau identifikuoti dirbtinį intelektą ir atitinkamai jį sureguliuoti.

Rekomendacijos

Kova su nusikaltimais yra vienas iš svarbiausių prioritetų užtikrinant veiksmingą keitimąsi informacija ir patirtimi tiek nacionaliniu, tiek Europos lygmenimis. Būtų galima numatyti galimybę išplėsti Europolo veiklą įtraukiant kibernetinę kriminalistiką ir stebėjimą.

Siekiant neatsilikti nuo kitų mokslų plačiai taikančių IT technologijas ir dirbančių su DI galimybių diegimą į savo sritis, kriminalistika privalo ne tik greitai ir sumaniai adaptuoti kitų mokslų pasiekimus ir per savo rekomendacijas pritaikyti juos nusikalstamų veikų aiškinimui, tyrimui ir prevencijai, bet

[57] Гросс, Г. (2002). *Руководство для судебных следователей как система криминалистики*. 16.

ir parengti ilgalaikes strategijas šių technologijų panaudojimui moksliniams ir taikomiesiems tikslams.

Kad kriminalistiniai duomenys būtų naudojami veiksmingai ir rezultatyviai, reikia suteikti galimybę dalytis dideliais duomenų kiekiais ir jais keistis, pasinaudojant dirbtinio intelekto priemonių kompiuterine galia, apdorojant ir naudojant tokius duomenis tarptautinių nusikaltimų aiškinimuisi. Vienas iš pavyzdžių – keitimasis duomenimis, stebint tarptautinius nusikaltėlius,

Kadangi dirbtiniu intelektu galima lengvai prekiauti tarptautiniu mastu, šioje srityje ilgalaikį poveikį užtikrintų tik pasaulinio masto sprendimai. G 7 ir G 20, Jungtinės Tautos ir Ekonominio bendradarbiavimo ir plėtros organizacija pradėjo nagrinėti dirbtinio intelekto vaidmenį, įskaitant jos vaidmenį karinėje srityje. ES toliau tokiuose forumuose skatins diskutuoti apie dirbtinį intelektą ir įvairius jo aspektus, įskaitant bendradarbiavimą mokslinių tyrimų ir inovacijų srityse ir konkurencingumą. Ji skatins naudoti dirbtinį intelektą ir apskritai visas technologijas, kad būtų lengviau spręsti pasaulinio masto problemas, įgyvendinti Paryžiaus klimato susitarimą ir siektiJungtinių Tautų darnaus vystymosi tikslų. ES gali ypatingu būdu prisidėti prie dirbtiniam intelektui skirtų pasaulinių debatų, remdamasi savo vertybėmis ir pagrindinėmis teisėmis.

ARTIFICIAL INTELLIGENCE AND DATA PROTECTION IN THE CONTEXT OF DEVELOPMENT OF CRIMINALSTICS

Jurgita Baltrūnienė

Summary

The article analyses how artificial intelligence (AI) is changing the way people live and work. Given the rapid development of AI technologies and the global political context, namely, the high level of investments in AI in an increasing number of the countries, the EU needs to work together to make the most of the many opportunities offered by AI and to address its challenges. Strengthening Europe's AI capacities is a key element in implementing a broader strategy aimed at ensuring that Europe adapts to the digital age and that the next 10 years become the digital decade, as set out in the Digital Compass. AI can be a strategic tool to address existing threats and anticipate both future risks, including hybrid threats, and opportunities. It can also contribute to the fight against crime and terrorism and enable law enforcement authorities to

keep track of the rapid development of technologies used by criminals and the ircross-border activities. We believe that the representatives of criminalistics do not yet pay enough attention to this issue. This should become one of the strategic directions for the development of criminalistics. AI can contribute to achieving the objectives of the EU Security Strategy.

Keywords: artificial intelligence (AI), European Union Internal Security Strategy, personal data, protection, privacy.