Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Kotrynos Seliutaitės
V kurso, tarptautinės ir Europos Sąjungos teisės
studijų šakos studentės

Magistro darbas

ES Bendrojo duomenų apsaugos reglamento taikymo dirbtiniam intelektui ypatumai

Vadovas: asist. dr. Julius Zaleskis

Recenzentė: lekt. dr. Gintarė Surblytė-Namavičienė

Vilnius
2020

TURINYS

ĮVADAS

Nagrinėjamos temos aktualumas. Moksliniais spėjimais iki 2021 m. 80 % naujų technologijų turės dirbtinio intelekto (**DI**) pagrindus[1]. Sparčiai besivystant ir plačiai pritaikant DI technologiją renkami ir naudojami neaprėpiami kiekiai asmens duomenų, kas neužtikrinant atitinkamų saugiklių ir priežiūros globaliu mastu kelia iššūkius asmenų teisėms į privatumą ir duomenų apsaugą. Turint omenyje, jog 90 % viso pasaulio duomenų buvo sukurti per pastaruosius penkerius metus[2], atitinkamas prisitaikymas reikalingas ir iš duomenų apsaugos reguliavimo perspektyvos. Šiame kontekste teisė turi pasitarnauti kaip kartu su žmonija evoliucionuojanti interesų derinimo priemonė, *inter alia* reikalinga sukurti stabdžius ten, kur interesų disbalansas gali kelti grėsmę tvariam visuomenės vystymuisi.

Nors investicijų į DI mastais Europos Sąjunga (**ES**) vis dar neprilygsta Jungtinėms Amerikos Valstijoms (**JAV**) ar Kinijai[3], ES išskiriama kaip viena svarbiausių pasaulinių žaidėjų technologijų reguliavime.[4] Ypatingas žingsnis duomenų apsaugos srityje žengtas priėmus ES Bendrąjį duomenų apsaugos reglamentą (**BDAR**)[5]. Sugriežtintos duomenų privatumo taisyklės ne tik pradėjo naują duomenų apsaugos reguliavimo etapą ES, bet kartu tapo pavyzdžiu bei atspirties tašku ir kitiems įstatymų leidėjams bei technologijų vystytojams visame pasaulyje.

DI kontekste daugiausia reikšmės sustiprintame BDAR reguliavime įgijo pritaikytosios ir standartizuotosios duomenų apsaugos bei automatizuoto sprendimų priėmimo, įskaitant profiliavimą kategorijos. Jų taikymas DI per trumpą laiką sukėlė daug diskusijų mokslinėje bendruomenėje, pradėta intensyviai leisti aiškinamąsias gaires, rekomendacijas ir kitus gerosios praktikos šaltinius (angl. *soft law)*. Tai rodo, kad abi nuostatos iš esmės apeliuoja į aktualius technologinius, inovacinius pokyčius. Visgi tai nėra vienintelės DI reikšmingos BDAR nuostatos – teisėtumo, sąžiningumo ir skaidrumo,

---

[1] JAIN, A., *et al*. 100 Data and Analytics Predictions Through 2022, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.gartner.com/en/documents/3875982/100-data-and-analytics-predictions-through-2022>.

[2] The Royal Society. *Machine learning requires careful stewardship says Royal Society*, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://royalsociety.org/news/2017/04/machine-learning-requires-careful-stewardship-says-royal-society/>.

[3] Žr. pvz. LOUCKS, J. *et al*. Future in the balance? How countries are pursuing an AI advantage, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www2.deloitte.com/us/en/insights/focus/cognitive-technologies/ai-investment-by-country.html>.

[4] Žr. pvz. SATARIANO, A., *et al*. Europe, Overrun by Foreign Tech Giants, Wants to Grow Its Own, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.nytimes.com/2020/02/19/business/europe-digital-economy.html>.

[5] 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. OL L 119, 2016.

duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo principai bei duomenų subjektams BDAR užtikrintos duomenų subjektų teisės būti pamirštam ar teisė į duomenų perkeliamumą taip pat daro itin didelę įtaką DI vykdomiems asmens duomenų tvarkymo procesams.

Visgi atskiri BDAR nustatyti reikalavimai yra vertinami nevienareikšmiškai – kai kurios BDAR nuostatos traktuojamos kaip sudėtingai suderinamos su DI technologija, ribojančios DI vystymąsi, kvestionuojamas jų tikslingumas ar praktinio pritaikomumo galimybės, kitos kritikuojamos dėl sudėtingos ir neaiškios teisinės formuluotės.

Siekdama išlikti konkurencinga DI srityje, ES turi rasti būdą, kaip suderinti savo suinteresuotumą duomenų apsaugos srityje su DI pažanga. O tam yra būtinas ne tik naujų teisėkūros metodų telkimas, tačiau ir mokslinis kuriamo reguliavimo tyrimas ir vertinimas.

Darbo tikslas. Šio darbo tikslas yra įvertinus DI reguliavimo asmens duomenų apsaugos kontekste poreikį ir priemones, identifikuoti BDAR taikymo DI prielaidas, ypatumus ir problematiką.

Darbo uždaviniai. Magistro darbo tikslui įgyvendinti tikslinga išspręsti šiuos uždavinius:

1) išskirti DI ir duomenų apsaugos bei privatumo kategorijas, atskleisti jų tarpusavio ryšį ir reguliavimo poreikį;
2) identifikuoti DI reguliavimo priemones ir pažangą asmens duomenų apsaugos kontekste ES, Lietuvoje ir JAV;
3) išnagrinėti esminius BDAR kaip DI reguliavimo šaltinio aspektus ir jo taikymo DI prielaidas;
4) išanalizuoti konkrečių BDAR principų ir normų taikymo DI ypatumus ir įvertinti BDAR reguliavimo suderinamumą su DI technologija.

Objektas. Darbo objektą lemia analizuojamai temai atskleisti išsikeltas tikslas bei uždaviniai. Objektą sudaro BDAR reguliavimo taikymas DI ir konkrečių BDAR normų taikymo DI problematika. Apsiribota esminių ir didžiausius iššūkius DI procesams keliančių nuostatų analize.

Struktūra. Darbą sudaro trys struktūrinės dalys. Pirmoje magistro darbo dalyje pirmiausia pristatoma DI apibrėžties problematika, privatumo ir duomenų apsaugos koncepcijų skirtis. Tuomet per DI ir duomenų apsaugos tarpusavio santykį atskleidžiamas asmens duomenis apdirbančio DI reguliavimo poreikis. Galiausiai įvertinama reguliavimo pažanga ir priemonės ES, nacionaliniu mastu Lietuvoje ir JAV. Antrojoje magistro dalyje dėmesys

sutelkiamas būtent į BDAR kaip duomenis apdirbančio DI reguliavimo šaltinį, aptariama esminės taikymo DI prielaidos ir reguliavimo bruožai. Trečiojoje darbo dalyje struktūriškai pirma vertinama BDAR numatytų duomenų apsaugos principų reikšmė DI, tuomet taikymo problematika analizuojama per konkrečias BDAR numatytas duomenų subjekto teises ir iš jų kylančias pareigas duomenų valdytojui ir tvarkytojui. Pažymėtina, jog autorės pasirinkimu darbe apsiribojama tik didžiausią problematiką DI reguliavimui keliančių BDAR aspektų analize, tikslingai vertinami ne visi reglamente nustatyti principai, duomenų subjektų teisės ir iš to kylantys reikalavimai.

Tyrimo metodai. Darbo tyrimo objektu esantys klausimai analizuojami pasitelkiant lingvistinį, teleologinį, sisteminį, istorinį ir lyginamąjį metodus. Pasitelkiant lingvistinį metodą BDAR nuostatų, *soft law* ir specialiosios literatūros šaltinių turinys aiškinamas per jų lingvistines formuluotes ir jų sudėtinius elementus. Naudojant teleologinį metodą sukurto reguliavimo turinys nagrinėjamas per įstatymų leidėjo siektą tikslą. Tai darbe aktualu turint omenyje aptakesnių ar kontraversiškai vertintinų BDAR nuostatų reikšmę ir tikslą. Sisteminis metodas pasitelktinas konkrečias įpareigojančias BDAR nuostatas vertinant neatsiejamai nuo visos BDAR normų ir principų sistemos, konstatuojamosios dalies punktų (**konst. d. p.**) bei susijusių *soft law* šaltinių. Lyginamasis metodas darbe nėra vienas pagrindinių, tačiau atskirais atvejais pasitelkiamas lyginant BDAR reguliavimą su pirmtake Duomenų apsaugos direktyva[6] (**Duomenų apsaugos direktyva**), lyginant ES ir JAV reguliavimo priemones, kurių aktualiai imtasi (nesiimta) siekiant sureguliuoti DI apdirbantį asmens duomenis bei lyginant atskiras BDAR nuostatose numatytas kategorijas ir jų sudėties elementus.

Istorinis metodas naudojamas DI koncepcijos formavimuisi nagrinėti ir teisės bei technologijų vystymuisi ir pažangai vertinti.

Svarbiausi šaltiniai. Atsižvelgiant į darbo temą pagrindinis analizuojamas šaltinis yra BDAR. Kadangi ES jurisdikcijoje kompetenciją turinčių teismų pozicijos BDAR normų taikymo konkrečiai DI atžvilgiu nėra suformuota, magistro darbe kaip teisės aiškinimo šaltiniais remiamasi *soft law* formuojamomis teisės aktų taikymo gairėmis bei pasaulio mokslininkų įžvalgomis moksliniuose darbuose ar straipsniuose. Teismų praktika pasitelkiama tik atskirų duomenų apsaugos aspektų vertinimui. Vertinant BDAR nuostatų

[6] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, OL L 281.

taikymo iššūkius DI, pateikiami skirtingi doktrinoje išsakomi socialinių ir technologijų mokslo atstovų ir praktikų požiūriai.

Daugiausia remiamasi autorių M. Brkan[7], L. A. Bygrave[8], M. Humerick[9], L. Mitrou[10], J. Zaleskio[11] moksliniais straipsniais ir monografijomis, Europos duomenų apsaugos valdybos (**EDAV**) (buvusios 29 straipsnio darbo grupės), Europos Komisijos sudarytos Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais (**DI ALEG**), Europos Komisijos (**EK**) parengtais *soft law* šaltiniais ir *traveaux preparatoires* medžiaga ir ypač BDAR. Be to, temos aktualumui atskleisti ir atskirais atvejais iliustraciniais tikslais taip pat pasitelktini statistikos šaltiniai, žiniasklaidos portalų publikacijos bei žymesnių visuomenėje praktinių atvejų, kompanijų ar prietaisų DI kontekste pavyzdžiai.

Pažymėtina, jog referuojant į šaltinius, pirmenybė teikiama tekstų turinio aiškinimui originalo kalba, todėl atitinkamai, nuorodos taip pat, esant poreikiui, tikslingai pateikiamos į dokumentą originalo kalba.

Darbo originalumas. Tarptautinės doktrinos kontekste tema aktualiai tirta daugiausia mokslinių straipsnių ar atskirų skyrių monografijose forma. M. Brkan straipsnyje „Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond“[12] analizuoja BDAR ir Teisėsaugos duomenų apsaugos direktyvos[13] (**Teisėsaugos direktyva**) automatizuoto sprendimų priėmimo taisykles ir nagrinėja kaip užtikrinti tokių sprendimų, ypač priimtų naudojant algoritmus, skaidrumą. L. A. Bygrave

[7] BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

[8] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, ir kt.

[9] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.

[10] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

[11] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019.

[12] BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

[13] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, OL L 119, 2016 5 4.

„Algorithmic Regulation“ skyriuje „Minding the Machine v2.0.“[14] nagrinėja BDAR 22 ir 25 straipsnius (**str.**) ir kaip šios nuostatos paveiks automatizuotas sprendimų priėmimo sistemas. M. Humerick komentare „Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence“[15] apžvelgia, kas yra DI ir kaip jis naudoja asmens duomenis vystymuisi, vertina kaip ES vaidmuo atitinkamame *amplua* mažėja, aptaria duomenų privatumą ir DI teisę ES, kaip naujos taisyklės gali neigiamai paveikti tvarų algoritminį vystymąsi, siūlo kaip ES turėtų pritaikyti savo požiūrį į duomenų privatumą ir apsaugą, kad būtų lengviau naudoti ir plėtoti DI. L. Mitrou darbe Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?[16] apžvelgia ir įvertinta DI aplinkai svarbias BDAR nuostatas susijusias su taikymo apimtimi, teisėtumo pagrindu, duomenų apsaugos principų taikymu bei naujomis atskaitomybės priemonėmis. Lietuvoje, autorės žiniomis, BDAR taikymo DI tema doktrinoje nėra tirta.

Duomenų apsaugos teisę nagrinėjančių mokslo darbų Lietuvoje yra rašyta, Vilniaus universiteto bendruomenėje ypač išskirtina I. Petraitytės daktaro disertacija tema „Asmens duomenų teisinės apsaugos principai“[17] ir J. Zaleskio monografija „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“[18]. Pastarojoje atskirais aspektais nagrinėtas ir duomenų apsaugos teisės aktualumas technologijų kontekste. Mykolo Romerio universitete apsiginta disertacija tema „Duomenų subjekto teisės virtualiuose socialiniuose tinkluose”[19].

Šis magistro darbas iš nagrinėtos tarptautinės mokslinės doktrinos išsiskiria BDAR reguliavimo taikymo DI tyrimo apimtimi ir naujumu. Darbe detaliai analizuojami visi reikšmingiausi BDAR DI taikymo aspektai ir pats BDAR DI taikymo kontekstas, lyginant ir sistemiškai vertinant skirtinguose aktualiausiuose mokslo šaltiniuose išdėstytą problematiką taip identifikuojant esminius BDAR DI taikymo ypatumus. Nors pagrindiniai

[14] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, ir kt.
[15] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[16] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) ‘Artificial Intelligence-Proof’?*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.
[17] PETRAITYTĖ, I. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
[18] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019.
[19] MALINAUSKAITĖ-VAN DE CASTEL, I. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius, Mykolo Romerio universitetas, 2017.

panašią temą tiriantys tarptautinės doktrinos šaltiniai yra parašyti 2018-2019 metais, turint omenyje aktualius aktyviai ES priimamus sprendimus DI reguliavimo kontekste, naujai išleistų *soft law* šaltinių bei mokslinių straipsnių gausą, akivaizdu, jog atitinkamoje šaltinių sudėtyje ir ES sprendimų kontekste tema dar nebuvo nagrinėta. Tai lemia skirtingos apimties darbo objektą ir kitu pagrindu prieitinas išvadas.

Lietuvoje panašia tema nagrinėjant DI ir duomenų apsaugos reguliavimą yra parašytas A. Aiduko 2018 m. Vytauto Didžiojo universitete apgintas magistro darbas tema „Data Privacy and Artificial Intelligence: Is General Data Protection Regulation the Right Regulation in the Age of Intelligent Machines?" ir Vilniaus universiteto absolventės A. Babayan 2018 m. darbas tema „Dirbtinio intelekto iššūkis žmogaus teisių apsaugos sričiai: robotų statuso reguliavimas". Lyginant atitinkamų autorių darbus su šiuo magistro darbu, skiriasi darbų tikslas, tikslui pasiekti keliamų uždavinių apimtis ir pasitelkiami šaltiniai.

1 DIRBTINIO INTELEKTO IR DUOMENŲ APSAUGOS TARPUSAVIO RYŠYS IR REGULIAVIMO PRIEMONĖS

1.1 Tarpusavio sąlyčio taškas

Dėl milžiniško kompiuterinės galios padidėjimo, gerokai sumažėjusių duomenų saugojimo išlaidų ir ilgus metus trukusių sudėtingų DI inžinierių ir mokslininkų tyrimų, visas DI potencialas pagaliau įgyja praktinę reikšmę. Tam ypač pasitarnavo per pastaruosius 10 metų dėl techninės įrangos pažangos (grafikos apdorojimo įrenginių – angl. *graphics processing unit*) ir dėl tokių kompanijų kaip „Facebook“ ir „Google“ paviešinto atvirojo kodo (angl. *open source*) ypač išpopuliarėjęs gilusis mokymasis (angl. *deep learning*), kaip mašininio mokymosi sritis ir DI vystymosi dalis. Daugelis kasdien naudojamų internetinių programų – pradedant „Google“ paieška, „Facebook“ ir „Netflix“, baigiant apsipirkimu internete „Amazon“ – naudoja DI metodus, kad geriau aptarnautų vartotoją. Išvados apie asmenis daromos remiantis vartotojų pačių pateikta informacija ir susikurtais individualiais profiliais, elgesiu viešojoje erdvėje bei vartotojų grįžtamuoju ryšiu, atsakomaisiais veiksmais reaguojant į DI sprendimus, kuris mašininiu mokymusi leidžia dar geriau nuspėti tolimesnį subjekto elgesį.[20] Visai automobilių pramonei sekant „Google“ pavyzdžiu, kuriami savaeigiai automobiliai, ir lėtai (pusiau) savarankiškai besivairuojančios transporto priemonės jau išrieda į viešus kelius. Vis dažniau šalia paplitusių pramoninių robotų visuomenėje rasis protingi pagalbininkai – tarnybiniai robotai, globos robotai, chirurgai-robotai, toliau plis DI pagrindu prijungti prie interneto veikiantys – aplinkos intelektas (angl. *ambient intelligence*), daiktų internetas (angl. *internet of things*), visuotinė kompiuterizacija (angl. *ubiquitous computing*) ar išmaniųjų namų (angl. *smart home*) sensoriai.

Norint DI atlikti bet kokią užduotį, šiems prietaisams reikia įvesties. Ne tik iš jų fizinės aplinkos, bet ir iš jų naudotojų. Prietaisai apdoroja informaciją, gaunamą iš savo naudotojų, sutelkiamą apie savo naudotojus ir naudotojus supančią / veikiančią informaciją.[21] Tokio plataus spektro informacijos apie asmenis apdirbimas reikalauja atitinkamų teisinių priemonių subjektų teisėms apsaugoti.

[20] Įprastas DI veiklos pavyzdys yra „Google“ paieškos pasiūlymai. Dažnai pakanka kelių raidžių įvesties, kad paieškos sistemos laukelyje būtų pateikiama pasiūlymų, ko ketinama klausti „Google“.
[21] NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018, p. 280-281.

Šiame skyriuje tiriamas DI santykis su teise ir reguliavimo poreikis. Dėmesys sutelkiamas į privatumo teisės ir duomenų apsaugos teisės sritis. Pirmiausia aptariama DI apibrėžties problematika, tuomet pagrindinės teisinės kategorijos: privatumas ir duomenų apsauga. Galiausiai, bus aptarta duomenų apsaugos ir privatumo santykis su DI technologijomis.

1.1.1 Dirbtinio intelekto koncepcijos raida ir apibrėžties problematika

DI vystymosi istorija prasidėjusi XX a. antroje pusėje[22] mokslininkų bendruomenėje lig šiol nepateikė visuotinai pripažintinos DI definicijos. Visgi iškart pažymėtina, jog šiuo darbu ir nesiekiama atrasti ar išvesti visuotinai pritaikytinos DI teisinės sąvokos – nagrinėjimo objektas yra DI apibrėžtumo problematika – kiek su ja susiduriama įstatymų leidybos prasme, siekiant implikuoti DI kategoriją į priimtiną reguliavimo sistemą.

Kitaip nei iš pirmo žvilgsnio gali pasirodyti, sudėtingumas apibrėžti DI, viena vertus, slypi ne intelekto „dirbtinume“, tačiau pačioje intelekto konceptualioje dviprasmybėje.[23] Kadangi žmonės yra vieninteliai subjektai, visuotinai pripažįstami (bent jau tarp žmonių) kaip turintys intelektą, nenuostabu, kad intelekto apibrėžimai paprastai ir siejami su žmogaus savybėmis. Vėlyvasis DI pradininkas John McCarthy, plačiai pripažintas kaip sukūręs terminą „dirbtinis intelektas“, teigė, jog „*nėra tvirtos intelekto apibrėžties, kuri nepriklausytų nuo jo sąsajų su žmogaus intelektu*“, nes „*mes dar negalime bendrai apibūdinti, kokias skaičiavimo procedūras norime vadinti protingomis*“.[24] Intelekto apibrėžimai labai skiriasi ir orientuojasi į daugybę tarpusavyje susijusių žmogaus

[22] JAV Dartmuto koledže 2006 m. buvo pakabinta lentelė, kurioje rašoma: „*Šiame pastate 1956 m. vasarą John Dartmouth (Dartmuto koledžas), Marvin L. Minsky (MIT), Nathaniel Rochester (IBM) ir Claude Shannon („Bell Laboratories“) vedė „Dartmouth dirbtinio intelekto vasaros tyrimų projektą“. Pirmasis sąvokos „Dirbtinis intelektas“ panaudojimas. Dirbtinio intelekto, kaip mokslo disciplinos, įkūrimas, siekiant tęsti prielaidą, kad kiekvienas mokymosi aspektas ar bet kuri kita intelekto ypatybė iš principo gali būti taip tiksliai apibūdinta, kad mašina gali būti sukurta ją imituoti.*““ Lentelėje įtvirtinta standartinė DI istorijos esmė – definicija gimė 1955 m., kai šie ankstyvosios karinės kompiuterijos veteranai kreipėsi į Rokfelerio fondą dėl vasaros stipendijos, skirtos finansuoti seminarą, kuris įgijo istorinę reikšmę DI disciplinos vystymesi. Lentelėje taip pat cituojama pagrindinė jų pasiūlymo koncepcija: kad protingą žmogaus elgesį sudaro procesai, kuriuos galima įforminti ir atgaminti mašinoje. DICK, S. Artificial Intelligence. Harvard Data Science Review, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://hdsr.mitpress.mit.edu/pub/0aytgrau>.

[23] SCHERER, M. U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology,* Volume 29, Number 2, Review, 2016 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>.

[24] See MC CARTHY, J. *What is Artificial Intelligence?* Computer Science Department Stanford University, 2007 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://perma.cc/U3RT-Q7JK>.

savybių, kurias pačiam sunku apibrėžti – įskaitant sąmoningumą, savimonę, kalbos vartojimą, gebėjimą mokytis, gebėjimą abstrakčiai suvokti, gebėjimą prisitaikyti ir protauti.

Kita vertus, yra ir daugiau problemų, susijusių su pakankamo apibrėžimo paieškomis. DI apibrėžimą sofistikuoja tai, jog spartus technologijų tobulėjimas *per se* neleidžia brėžti griežtų ribų su laiku pažangumo prasme save peraugančiai ir nuolat besivystančiai DI kategorijai. Net jei sutiktume, kad sistemai pavadinti DI reikia tam tikro intelekto lygio, sunku nustatyti kam tiksliai taikytume šią apibrėžtį, pvz., kalbant apie sudėtingą DI sistemą, apimančią daugybę modulių, programų ir paprogramių – kvestionuotina – ar kiekvienas iš šių elementų savaime laikomas DI, ar taip yra tik tada, kai jie veikia kaip visuma. Panašūs klausimai kyla, kai keli kompiuteriai dirba tarpusavy kartu arba kartu su papildomomis programomis, kurios gali intelektualiai apdoroti informaciją, bet taip pat gali atlikti ir intelekto nereikalaujantį „kvailąjį“ apdorojimą.[25]

Atsižvelgiant į probleminius aspektus, gali pasirodyti, jog beveik neįmanoma pasiekti vieningos DI apibrėžties. Visgi yra siūlymų, kad į „kvailąsias“ programas, „botus“, DI (taip pat susijusias technologijas) ir t. t. geriau žiūrėti ne kaip į atskirai apibrėžtų kategorijų, turinčių aiškias ribas, rinkinį, bet kaip į galimo intelekto skalės lygius – tokiu būdu diskusija būtų ne „kaip nubrėžti griežtą ribą tarp to, kas yra ar nėra DI“, o „kas gali perkelti programą ar programų rinkinį aukštyn ar žemyn skalėje“ ir „ties kuriais skalės taškais paprastai pradedame vadinti daiktus DI?“[26].

Aktualiai DI apibrėžties problematika jau bandyta spręsti ES mastu. Pirma DI apibrėžtis pasiūlyta EK komunikate „DI Europai“[27], ilgai netrukus po jos pasirodymo, EK sudarytos DI ALEG iniciatyva, referuojant į aukščiau minėtą EK komunikatą, definicija vystyta atskirame dokumente „DI apibrėžtis“[28]. Palyginus pateiktas sąvokas, DI ALEG

---

[25] WRIGLEY, S. Bots, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199, 2019, p. 202-203 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą:
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>.

[26] *Ibid*. p. 203.

[27] „*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).*“ Žr. 2018 m. balandžio 25 d. Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Dirbtinis intelektas Europai, COM/2018/237 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/LT/COM-2018-237-F1-LT-MAIN-PART-1.PDF>.

[28] „*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 – analizuoja savo aplinką rinkdamos duomenis, aiškina surinktus struktūruotus ir nestruktūruotus duomenis,*

pasiūlyta definicija yra platesnė ir be analogiškų elementų papildomai apima tokius aspektus kaip kad DI sistemos (i) yra būtent žmonių sukurtos, (ii) detalizuojama, jog geba aiškinti tiek struktūrizuotus, tiek nestruktūrizuotus duomenis, (iii) gali veikti naudojant simbolines taisykles arba sudaryti skaitmeninį modelį ir, ypač svarbu, kad išskiriamas aspektas, jog DI sistemos (iv) koreguoja savo elgesį. Be kita ko, atkreiptinas dėmesys, kad DI ALEG be pačios sąvokos išskiria DI ne tik kaip sistemą, tačiau atskirai ir kaip mokslo šaką. Toks definicijos ribų išplėtimas, galima vertinti, jog atspindi siekį reguliavimu kuo labiau atspindėti aktualų DI technologijos modelį ir pažangos lygį, tiklsiau identifikuoti „intelektualiajai“ sistemai būdingas savybes, siekiant jas išskirti iš kitų (atitinka Wrigley, Sam siūlomą DI apibrėžties orientavimą į intelekto pažangos lygį). Visgi, darbo autorės nuomone, toks identifikuojančių sudedamųjų plėtimas tuo pačiu griežtina DI ribas, kas, turint omenyje sparčią technologijų pažangą, gali būti rizikinga ir netvaru reguliavimo prasme[29].

Spręsti DI apibrėžties problematiką yra svarbu todėl, kad bet koks reguliavimas turi pirma atsakyti į klausimą – kas tiksliai juo reguliuojama. Vienas iš pagrindinių būsimos specialios DI reglamentavimo sistemos klausimų ir bus nustatyti jos taikymo aprėptį. Visgi, kaip rašoma aktualiai priimtoje Baltojoje knygoje, bet 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.[30]

Šiame darbe definicijos klausimas spręstinas darbo tikslais apibrėžiant DI aptakiu bendriniu būdu: „dirbtinis intelektas“ – tai mašinos, galinčios atlikti užduotis, kurios, jei jas atlieka žmogus, reikalauja intelekto. DI sistema, paremta šiuolaikine skaitmenine kompiuterija, apima ir techninės, ir programinės įrangos komponentus, todėl terminu DI toliau gali būti referuojama į robotą, programą, veikiančią viename kompiuteryje,

---

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 sudaryti skaitmeninį modelį, jos taip pat gali koreguoti savo elgesį analizuodamos, kokį poveikį aplinkai padarė jų ankstesni veiksmai. Kaip mokslo šaka, DI apima keletą metodikų ir metodų, pavyzdžiui, mašinų mokymąsi (konkretūs pavyzdžiai – gilusis mokymasis ir sustiprintas mokymasis), mašinų atliekamą loginę analizę (įskaitant veiksmų ir laiko planavimą, žinių vaizdavimą, loginę analizę, paiešką ir optimizavimą) ir robotiką (įskaitant kontrolę, suvokimą, jutiklius, veiksmo mechanizmus ir visų kitų metodų integravimą į kibernetines - fizines sistemas)“. Žr. 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Definition of AI: Main Capabilities and Disciplines [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

[29] Nors ir turint omenyje, jog abu šie aktai yra tik *soft law* šaltiniai, t. y. neprivalomo taikymo.

[30] 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final, p. 17 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.

programą, veikiančią tinklais sujungtuose kompiuteriuose (angl. *networked computers*), arba bet kurį kitą komponentų rinkinį, kuriame yra DI.

1.1.2 Privatumas ir duomenų apsauga

Nagrinėjant DI ryšį su privatumu ir duomenų apsauga pirmiausia pažymėtina, jog privatumas ir duomenų apsauga yra dažnai painiojamos atskiros kategorijos. Nors iš dalies jos ir persidengia, vis dėl to turi skirtingą prasmę. Svarbu jas atskirti, nes tai, kas duomenų apsaugos atžvilgiu gali būti visiškai teisėta, vis tiek gali būti privatumo pažeidimu, galinčiu rimtai paveikti asmenis.[31]

1.1.2.1 Privatumas

„*Iš visų tarptautiniame žmogaus teisių rinkinyje įtvirtintų teisių turbūt sunkiausia yra apibrėžti privatumą*“ – Norman S. Marsh.[32]

Privatumas yra *slidi* sąvoka, dažnai ir lengvai vartojama, tačiau jos tiksli reikšmė toli gražu nėra aiški.[33] Ankstyvas nuorodas į privatumo pažeidimus ir apsaugą galima rasti net gi Biblijos ištraukose. Bet kuris asmuo, pažeidęs ar įsibrovęs į kažkieno privatų gyvenimą, buvo vertinamas su pykčiu ir gėda. Hamurabio teisyne taip pat užsiminta apie įsibrovimą į kieno nors namus. Teisė į privatumą buvo ginama ir hebrajų kultūroje, senovės Graikijoje ir Kinijoje.[34]

Pažymėtina, jog be kita ko, net ir pats privatumas, lyginant su teise į privatumą, nėra tapačios sąvokos. Privatumas tai objektas, gėris, vertybė, o teisė į privatumą – tai teisinė kategorija – subjektinė teisė į privatumo gynybą ir šios teisės turinys.

Kalbant apie žmogaus teises, privatumas yra palyginti naujas apsaugos objektas. Nors privatumo sąvoka turėjo pirmtakų daugelio skirtingų teisinių sistemų doktrinose, advokatas Samuel D. Warren ir JAV aukščiausiojo teismo teisėjas Louis Brandeis plačiai

---

[31] DE CONCA, S., *et al*. Artificial intelligence and privacy: DI enters the house through the cloud, 2018, iš W. Barfield, & U. Pagallo Eds NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018, p. 282.

[32] MARSH, N. S., Privacy and Human Rights. By James Michael. *International and Comparative Law Quarterly*, British Institute of International and Comparative Law, 1995 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/privacy-and-human-rights-by-james-michael-dartmouth-unesco-publishing-1994-ix-135-text-55-appendices-and-index-pp-isbn-1855213818-5795/BA80F717E512CF28193AB21693582145#>.

[33] KOOPS, B., *et al*. 'Code' and the Slow Erosion of Privacy, *Michigan Telecommunications and Technology Law Review*, Volume 12, 2005 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr`>.

[34] ABHAY, J. S., *et al*. Artificial Intelligence: A Threat to Privacy. *Nirma University Law Journal*, vol. 8, no. 2, 2019, p. 25 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline-org.ezproxy.vdu.lt:2443/HOL/Page?handle=hein.journals/nulj8&id=139&collection=journals&index=>.

pripažįstami pirmaisiais iškėlusiais mintį, kad privatumas yra teisė, verta teisinės apsaugos. Garsiajame 1890 m. „Harvard Law Review“ Brandeis privatumas apibrėžtas kaip „teisė būti paliktam vienu“[35]. Šis apibrėžimas jau rodo, kad privatumas yra gana plati kategorija. „Palikimas vienu“ galimas įvairiose situacijose: erdvinėse, fizinėse, komunikacinėse, santykinėse, informacinėse.

Europos žmogaus teisių konvencijos (**EŽTK**) 8 str., kuris paprastai laikomas viena iš šiuolaikinio (Europos) privatumo reguliavimo šaknų, teigiama, kad „*kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas*“. Tai vėlgi pabrėžia skirtingus privatumo aspektus. Be to, teisė į privataus gyvenimo gerbimą buvo ir tebėra saugoma kaip bendrasis ES teisės principas pagal Europos Sąjungos Teisingumo Teismo (**ESTT**) praktiką.[36]

Po 1967 m. Westino teorijos, ryškesniu tampa informacinis privatumo aspektas ir privatumas jau apibrėžiamas kaip „individų, grupių ar institucijų reikalavimas patiems nustatyti, kada, kaip ir kokiu mastu informacija apie juos perduodama kitiems asmenims“.[37] Naujesnis aiškinimas, ką reiškia ar bando apsaugoti privatumas, remiasi Westino kontrolės sąvoka ir yra įrėmintas profiliavimo, socialinės žiniasklaidos, interneto kontekste.[38]

Galiausiai 2002 m. Lee A. Bygrave tarptautinės doktrinos pateikiamus privatumo apibrėžimus pasiūlo suskirstyti į keturias grupes[39], kuomet privatumas apibrėžiamas kaip (i) nesikišimas į asmens gyvenimą; (ii) prieigos prie asmens ribojimas; (iii) asmenų atliekama informacijos apie juos kontrolė ir (iv) intymių ir jautrių asmens gyvenimo aspektų apsauga.[40]

---

[35] WARREN, S. D. and BRANDEIS, L. D. The Right to Privacy, *Harvard Law Review*, vol. 4, No. 5, 1890 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <www.jstor.org/stable/1321160>.

[36] Europos Sąjungos Teisingumo Teismas. *1980 m. birželio 26 d. sprendimas byloje 136/79 National Panasonic (UK) Limited prieš Europos Bendrijų Komisiją, EU:C:1980:169*, p. 17 et seq., Europos Sąjungos Teisingumo Teismas. *1992 m. balandžio 8 d. sprendimas byloje C-62/90 Komisija prieš Vokietiją, EU:C:1992:169*, p. 23.

[37] WESTIN, A. E., Privacy and Freedom, *Washington and Lee Law Review*, Volume 25 Issue 1, 1968, p. 166 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.

[38] TREPTE, S., et al., *Privacy Online – Perspectives on Privacy and Self-Disclosure in the Social Web*, 2011 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://books.google.lt/books?id=ru2aU0r7sM0C&pg=PA10&lpg=PA10&dq=Westin+1967+AI&source=bl&ots=BLvLjgV-HI&sig=ACfU3U0dOS38HhprUjzDnPc3VRSAeVNJjA&hl=lt&sa=X&ved=2ahUKEwiLn4Ov2J_oAhVh-SoKHdXXD6gQ6AEwAXoECAkQAQ#v=onepage&q&f=false>.

[39] BYGRAVE, L. A. *Data protection law. Approaching its rationale, logic and limits*. Dordrecht: Kluwer law international, 2002, P. 128-129 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/220668128_Data_Protection_Law_Approaching_its_Rationale_Logic_and_Limits_by_L_A_Bygrave>.

[40] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 38.

Pastebėtina, jog skirtingose privatumo „interpretacijose“ Warren ir Brandeis atvejais sampratos turinys formuluojamas iš skirtingų subjektų perspektyvos – (i) informacijos rinkėjų, kurie gali rinkti duomenis skirtingose aplinkose Warren ir Brandeis atveju arba (ii) pačių informacijos davėjų (Westino atveju).[41] Kuomet Lee A. Bygrave siūlomas apibrėžimas – formuluojamas tiek iš proaktyvaus duomenų subjekto, tiek informacijos rinkėjų perspektyvos, tiek ir orientuojantis į pačią privatumo kategoriją, taigi orientuojama ir į patį objektą, pvz. jautrius gyvenimo aspektus.

Lyginant skirtingus diktuojamus privatumo konceptus ar konceptų kategorijas, akivaizdu, jog visuomenėje ir mokslinėje bendruomenėje nėra visiems bendro supratimo, ką reiškia privatumas. Galima numanyti, jog interpretacijos laikui bėgant kinta tiek dėl technologijų pažangos, dėl kurios privačioje erdvėje tampa aktualūs skirtingų formų pažeidimai, tiek dėl besikeičiančios viešosios nuomonės bei vertybinių orientyrų pokyčių.

1.1.2.2 Duomenų apsauga ir ryšys su privatumu

„*Duomenų apsaugos teisės saugomas privatumas yra pagrindinė žmogaus teisė ir konstitucinė vertybė pagarba asmeniui grįstoje visuomenėje*“ – rašo Julius Zaleskis[42].

Privatumas, lyginant su duomenų apsauga, yra paprastai laikytinas labiau apimančia koncepcija. Ieškant sąsajos tarp privatumo ir duomenų apsaugos gali būti teigiama, jog žmogaus privataus gyvenimo neliečiamumas sudaro asmens duomenų apsaugos teisinio reguliavimo branduolį[43], t. y. teisės į privatumą apsauga suvokiama kaip duomenų apsaugos teisės tikslas. Kadangi privatumas, o kartu ir duomenų apsauga, yra laikomos pagrindinėmis teisėmis, yra daug teisinių nuostatų, kuriomis apibrėžiamos ir saugomos šios teisės, tačiau teisių taikymo sritis ir konkretus privatumo ir duomenų apsaugos reglamentavimas skiriasi.

---

[41] DE CONCA, S., *et al*. Artificial intelligence and privacy: DI enters the house through the cloud, 2018, iš W. Barfield, & U. Pagallo Eds NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018. P. 282-283.

[42] ZALESKIS, J. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 39.

[43] PETRAITYTĖ, I. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79, p. 135 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330722412_Asmens_duomenu_apsaugos_teisinis_reguliavimas_Lietuvos_teises_sistemoje>.

Privatumas, kaip pagrindinė žmogaus teisė pasaulyje buvo pripažinta: Visuotinėje žmogaus teisių deklaracijoje[44], Tarptautiniame pilietinių ir politinių teisių pakte[45], Vaiko teisių konvencijoje[46] ir Tarptautinėje visų migruojančių darbuotojų ir jų šeimų narių apsaugos konvencijoje[47], Konvencijoje dėl žmonių su negalia teisių[48]; regioniniu lygmeniu teisė ginama pagal: Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją (**EŽTPLAK**)[49], ES pagrindinių teisių chartiją[50] (**Chartija**) ir Amerikos žmogaus teisių konvenciją[51], Kairo deklaraciją dėl žmogaus teisių Islame[52], Arabų žmogaus teisių chartiją[53], Afrikos chartiją dėl vaiko teisių ir gerovės[54], Azijos ir Ramiojo vandenyno šalių ekonominio bendradarbiavimo organizacijos privatumo sistemą. Kuomet į duomenų apsaugą orientuotos nuostatos pagrinde įtvirtintos tik Chartijoje[55], Europos Tarybos konvencijoje dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[56] ir BDAR.

Kaip matyti, priešingai nei EŽTPLAK, kurioje nėra atitinkamos nuostatos dėl duomenų apsaugos, Chartijos 8 str. duomenų apsauga ne tik atskiriama nuo privatumo, bet ir 2 ir 3 dalyse nustatomos tam tikros konkrečios garantijos, būtent, kad asmens duomenys turi būti tvarkomi sąžiningai konkrečiais tikslais ir remiantis atitinkamo asmens sutikimu

---

[44] 1948 m. gruodžio 10 d. Visuotinė žmogaus teisių deklaracija, *Valstybės žinios*, 2006-06-17, Nr. 68-2497, 12 str.

[45] 1966 m. gruodžio 19 d. Tarptautinis pilietinių ir politinių teisių paktas, *Valstybės žinios*, 2002-08-02, Nr. 77-3288, 17 str.

[46] 1989 m. lapkricio 20 d. Vaiko teisių konvencija, *Valstybės žinios*, 1995-07-21, Nr. 60-1501 16 str.

[47] 1990 m. gruodžio 18 d. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, 14 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CMW.aspx>.

[48] 2009 m. balandžio 24 d. Europos Parlamento rezoliucija dėl Jungtinių Tautų konvencijos dėl žmonių su negalia teisių ir jos fakultatyvinio protokolo pasirašymo Europos bendrijos vardu, 22 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:184E:0111:0113:LT:PDF>.

[49] 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, iš dalies pakeista protokolais Nr. 11 ir 14, su Pirmuoju Protokolu ir papildomais protokolais Nr. 4, 6, 7, 12, 13 ir 16, 8 str.

[50] 2016 m. birželio 7 d. Europos Sąjungos pagrindinių teisių chartija, 2016/C 202/02, OL C 202, 2016 6 7, 7 str.

[51] 1969 m. lapkričio 22 d. American Convention on Human Rights, 11 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm>.

[52] 1990 m. rugpjūčio 5 d. Cairo Declaration on Human Rights in Islam, 18 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.refworld.org/docid/3ae6b3822c.html>.

[53] 1994 m. rugsėjo 15 d. Arab Charter on Human rights, 17 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www.humanrights.se/wp-content/uploads/2012/01/Arab-Charter-on-Human-Rights.pdf>.

[54] 1990 m. liepos 1 d. African Charter on the Rights and Welfare of the Child, OAU Doc. CAB/LEG/24.9/49, 10 str. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.un.org/en/africa/osaa/pdf/au/afr_charter_rights_welfare_child_africa_1990.pdf>.

[55] 8 str.

[56] 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis, *Valstybės žinios*, 2001-04-13, Nr. 32-1059, 1 str.

ar kokiu nors kitu teisėtu įstatymu nustatytu pagrindu; kad kiekvienas asmuo turi teisę susipažinti su surinktais duomenimis ir teisę juos ištaisyti; ir kad šių taisyklių laikymąsi kontroliuoja nepriklausoma institucija. Taigi jau iš Chartijos nuostatų, susijusių su privatumu ir duomenų apsauga, matyti, kad šios dvi teisės nėra sinonimas.[57]

Nepaisant Chartijos nustatyto privatumo ir duomenų apsaugos atskyrimo, teismų praktikoje privatumas laikomas duomenų apsaugos pagrindu.[58] Tiek ESTT, tiek Europos Žmogaus Teisių Teismo nuomone, sąvoka „privatus gyvenimas“ neturi būti aiškinama ribotai. ESTT EŽTT praktiką aiškina taip, kad „privatus gyvenimas“ apima asmens duomenų apsaugą, kuri apibrėžiama kaip bet kokia informacija, susijusi su identifikuotu ar identifikuojamu asmeniu.[59] Atitinkamai, tokiu ryšiu siejant subjektines teises galima aiškinti, kad teisė į duomenų apsaugą traktuotina kaip teisės į privatumą elementas.

175 pasaulio šalys[60], tarp jų ir Lietuva[61], pripažino teisę į privatumą ir savo Konstitucijoje, kitos, kaip antai JAV[62], Airija[63], Prancūzija[64] – savo Konstitucijoje privatumo aiškiai nenurodė. Visgi viso pasaulio šalys stengėsi priimti išsamius privatumo įstatymus, o daugelis įstatymų grindžiami EBPO ir Europos Tarybos priimtais modeliais. Įsigaliojusiame BDAR iš esmės išryškinta asmens duomenų apsaugos reikšmė. Net gi ES nepriklausančios šalys tuo pasinaudojo ir priėmė privatumo įstatymus. Atkreiptinas dėmesys, kad daugelis šalių vis dar priiminėja, ir tik daugiau kaip keturiasdešimt šalių jau yra priėmusios duomenų apsaugos arba informacijos privatumo įstatymus.[65]

---

[57] KOKOTT, J. *et al*. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, 2013, Vol. 3, No. 4 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/275199054_The_distinction_between_privacy_and_data_protection_in_the_jurisprudence_of_the_CJEU_and_the_ECtHR>.

[58] *Ibid*.

[59] Europos Sąjungos Teisingumo Teismas. *2010 m. lapkričio 9 d. sprendimas sujungtose bylose Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen, EU:C:2010:662*, p. 52.

[60] Comparative Constitutions Project [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.constituteproject.org/search?lang=en&key=privacy&status=in_force>.

[61] 1992-10-25 Lietuvos Respublikos Konstitucija, *Lietuvos aidas*, 1992-11-10, Nr. 220-0, 22 str.

[62] U. S. Constitution, the Bill of Rights & All Amendments [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://constitutionus.com>.

[63] Constitution of Ireland with all amendments, 1937 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.gov.ie/en/publication/d5bd8c-constitution-of-ireland/>.

[64] Constitution de la France, du texte intégral en vigueur, 1958 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur>.

[65] JAIN, S. *et al*. Artificial intelligence: threat to privacy. *Nirma University Law Journal*, 8(2), 2019, p. 26-28 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nulj8&div=16&id=&page=>.

1.1.3 Dirbtinio intelekto ir duomenų apsaugos sąlyčio taškas

EK Baltojoje knygoje, kartu referuojant ir į visas galimas diskusijas dėl politikos iniciatyvų ateityje, pagrindiniais DI elementais išskiriami „duomenys“ ir „algoritmai“. Pats DI technologijos pobūdis reiškia duomenų naudojimą. Be duomenų, nėra DI[66], duomenys yra mašininio mokymosi žaliava. Nepriklausomai nuo to, koks algoritmas yra naudojamas, jiems visiems reikalingas didelis informacijos kiekis, kad būtų galima apdoroti, išgauti modelius ir sukurti profilius, kurie, suteiks programinei įrangai pakankamai informacijos, su tikslu išmokti ir nuspręsti, kaip geriau atlikti tam tikras užduotis. Dėl šios aplinkybės DI vystymasis yra ypač susijęs su asmens duomenų apsaugos reguliavimu.[67]

Duomenų apsauga apima asmenų apsaugą, kai ji susijusi su informacija apie asmenis, ir todėl yra glaudžiai susijusi su informacinio privatumo sąvoka. Didelio kiekio duomenų apie individualų ir kolektyvinį elgesį generavimas, rinkimas, apdorojimas ir dalijimasis jais gali būti atliekamas pasitelkus DI. Asmens privatumui ir asmeniniam gyvenimui gali turėti neigiamos įtakos jo asmens duomenų rinkimas ir (arba) naudojimas. Galima analizuoti ir optimizuoti jutiminius duomenis, tokius kaip veido, balso įrašymo, gyvybingumo, individo DNR, kur kas greičiau ir geriau pasitelkus DI ir naudojant kompiuterinius algoritmus. Visgi viskas, kas yra vertinga ar gali sukelti žalą, neišvengiamai kels teisinius klausimus.[68] Dėl šios priežasties asmens duomenų rinkimas ir naudojimas, bent jau Europoje, yra gana griežtai reguliuojamas. Tie, kurie naudoja duomenis, ir tie, kurie naudoja automatinio mokymosi sprendimus, naudojančius duomenis, turi įsitikinti, kad naudojimas yra teisėtas ir nėra priežasčių atsakomybei kilti.[69]

DI tapo labai patrauklus dėl greičio, masto ir automatizavimo. Šios DI savybės, anot Dr. Sunitha Abhay Jain ir Simran A. Jain leidžia daryti poveikį privatumui įvairiais būdais:

1. Duomenų naudojimu. Didėjant pasitikėjimui DI technologijomis, didėja ir jų panaudojimo galimybės. Daugelis vartotojų produktų, pradedant išmaniaisiais buitiniais prietaisais ir baigiant kompiuterinėmis programomis, yra pažeidžiami DI

[66] 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.
[67] DE CONCA, S., *et al*. Artificial intelligence and privacy: DI enters the house through the cloud, 2018, iš W. Barfield, & U. Pagallo Eds NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018, p. 297.
[68] LOHR, J. D., et al. Legal Practitioners' Approach to Regulating AI Risks, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 231.
[69] *Ibid*.

duomenų naudojimo. Naudodamas DI, žmogus paprastai nesusižino, kiek duomenų jų programinė įranga ir įrenginiai realiai generuoja, apdoroja ar bendrina.

2. Identifikavimu ir sekimu. DI gali būti naudojamas siekiant identifikuoti, sekti ir stebėti asmenis keliuose įrenginiuose, nesvarbu, ar jie yra darbe, ar namuose, ar bet kurioje viešoje vietoje. Jei asmens duomenys yra anonimizuoti ir, kai jie tampa didelio duomenų rinkinio dalimi, DI gali panaikinti šių duomenų anonimiškumą, remdamasis kitų prietaisų padarytomis išvadomis. Tai panaikina skirtumą tarp asmeninių ir neasmeninių duomenų.
3. Balso ir veido atpažinimu. Asmenų privatumui ir anonimiškumui labai pakenkta, naudojant du identifikavimo metodus, kuriuos DI vis geriau taiko – balso atpažinimą ir veido atpažinimą. Pvz., veido atpažinimą ir balso atpažinimą teisėsaugos institucijos naudoja tyrimo tikslais ir nusikaltėlių sekimui.[70]
4. Numatymu. Norint nustatyti ar nuspėti neskelbtiną informaciją iš neskelbtinų duomenų formų, naudojami DI ir sudėtingi mašininio mokymosi algoritmai. Pvz., kieno nors klaviatūros spausdinimo raštus galima panaudoti savo emocinėms būsenoms, tokioms kaip nervingumas, pasitikėjimas savimi, liūdesys ir nerimas, išskaityti. Dar didesnį nerimą kelia tai, kad asmens politines pažiūras, etninę tapatybę, seksualinę orientaciją ir net bendrą sveikatą taip pat galima nustatyti pagal tokius duomenis kaip veiklos žurnalai, vietos duomenys ir panaši metrika.
5. Profiliavimu. Duomenys, surinkti naudojant DI, yra profiliuojami ir gali būti naudojami rūšiuoti, vertinti, klasifikuoti, reitinguoti žmones. Pagal blogą praktiką pasaulyje duomenys gali būti renkami ir paprastai negavus duomenų subjekto sutikimo. Kinijos socialinių balų sistema yra pavyzdys, kaip ši informacija gali būti naudojama ribojant galimybes naudotis kreditais, būstu, užimtumu ar socialinėmis paslaugomis.[71]

Kuomet vertinant duomenų poveikį DI – Jason D. Lohr, Winston J. Maxwell ir Peter Watts išskiria[72], jog DI naudojant asmens duomenis (i) įvesties duomenims gali būti taikomi apribojimai, todėl tvarkantieji asmens duomenis pasitelkdami mašininio mokymosi sprendimus turi įsitikinti, kad naudojimas yra teisėtas ir neprišauks teisinės atsakomybės taikymo; (ii) įvesties duomenys lems rezultatus, todėl nuo duomenų kokybės priklauso ne

[70] JAIN, S. *et al*. Artificial intelligence: threat to privacy. *Nirma University Law Journal*, 8(2), 2019, p. 33 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nulj8&div=16&id=&page=>.
[71] *Ibid*. p. 34
[72] LOHR, J. D., et al. Legal Practitioners' Approach to Regulating AI Risks, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 231-233.

tik DI konkretaus sprendimo priėmimas, tačiau ir ateities sprendimai, turint omenyje DI sistemų mokymąsi; (iii) įvesties duomenys gali padaryti algoritmą vertingesniu – įvedamos informacijos naudojimas apmokant DI sistemas kuria pridėtinę vertę sistemos modeliams ir jos ateities naudotojams; itin jautrių duomenų apdirbimo kontekste, autoriai klausimą, ar nėra reikalingi naujo tipo konfidencialumą užtikrinantys principai, nustatantys, kaip sukurta pridėtine verte turėtų būti dalijamasi tarp sistemų; (iv) galiausiai pažymima, jog tapatybės duomenys gali būti kuriami ir atvirkštine tvarka, t. y. net ir anonimizavus asmens duomenis, DI, apdirbantis daugybės asmenų profilius, gali net ir pašalinus asmenį identifikuojančius aspektus, kaip reikalaujama[73], daugybės asmens atliekamų veiksmų pagrindu sukurti ir atpažinti vienam unikaliam asmeniui būdingą profilį. Tai reiškia, jog yra rizika, jog reguliavimas iš esmės nėra pakankamas siekiant apriboti galimą grėsmę duomenų saugumui. Asmenį DI geba identifikuoti atgaline tvarka galimai formaliai nepažeidžiant galiojančių teisės aktų.

Taigi, galima teigti, jog sparti technologinė pažanga, atvėrusi galingos asmens duomenų rinkos galimybes, kelia būtinybę įstatymų leidėjui aktyviai reaguoti siekiant apsaugoti asmenų teises. Reikalinga užtikrinti tiek saugią erdvę silpnesniajai šaliai – duomenų subjektams kontroliuoti savo duomenis ir ginti savo teises, tiek erdvę technologijų kūrėjams ir verslo atstovams plėtoti išradimus ir lygiai taip būti saugiems teisių gynybos klausimais.

1.2 Asmens duomenis apdirbančio dirbtinio intelekto reguliavimas

Anot Matthew U. Scherer, ryšium su DI reguliavimu įstatymų leidėjui kyla dvejopo pobūdžio iššūkiai: (i) *ex ante* iššūkiai – DI tyrimų ir vystymo reguliavimo klausimai ir (ii) *ex post* iššūkiai – DI kūrimo ir implikavimosi visuomenėje reguliavimas.[74] Iš principo problematika tokiu atveju skiriama pagal iššūkius DI kūrimo ir taikymo etapuose. Kita vertus, pastebima, jog DI reguliavimą sofistikuoja ir (i) bet kokiam reguliavimo rėžimui reikalingos vieningos DI apibrėžties nebuvimas; (ii) konkrečiai DI reguliuojančio teisės akto / teisės aktų sąvado v. esamos įstatyminės bazės pritaikymo poreikio klausimas, (iii) DI subjektiškumas ir atsakomybės klausimai. Tokie aspektai yra aktualūs daugeliui DI

[73] BDAR 26 konst. d. p.
[74] SCHERER, M. U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology,* Volume 29, Number 2, Review, 2016, p. 359 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>.

reguliavimo sričių, tarp kurių yra ir duomenų apsauga. Turint omeny aktualią technologijų vystymosi spartą tai apspręsti pakankamai sudėtinga. Pagal tarptautinę praktiką, dažnu atveju kol kas galima pastebėti tik užuomazgas naujų teisės aktų, konkrečiai pritaikytų DI sistemoms reguliuoti. Visgi, sparti DI raida akivaizdžiai paskatino visuotines ir vietos diskusijas dėl DI valdymo. Pradėtos aktyviai rengti nacionalinės ir tarptautinės strategijos, reguliavimo problematikai spręsti formuotos darbo grupės, leisti teisės aktų aiškinimo komentarai.

Turint omeny šiame darbe analizuotiną DI reguliavimą ryšium su duomenų apsauga ir BDAR toliau autorė, nagrinėdama šaltinius, reguliuojančius DI ir duomenų apsaugos klausimus ES, nacionaliniu mastu ir JAV, bandys atsakyti į klausimą – ko lig šiol pasiekta duomenų apsaugos reguliavime, kuris atitiktų DI technologijos keliamus iššūkius ir technologinį pritaikomumą?

1.2.1 Reguliavimo teisinė bazė ES

ES buvo kritikuojama dėl to, kad „buvo trečia“ DI vystymo lenktynėse, gerokai atsilikusi tiek nuo JAV, tiek nuo Kinijos.[75] ES ne tik mažiau lėšų skyrė technologijų vystymui[76], bet kaip plačiai visuomenėje įprasta vertinti, sukūrė ir nelanksčią reguliavimo aplinką (BDAR, vartotojų teisė, e. privatumas ir kt.), kurioje prieiga prie duomenų yra sunkesnė, o eksperimentinis naudojimas – neteisėtas. Visgi, didėjant pasauliniam informuotumui apie privatumą ir skaidrumą (pvz., Cambridge Analytica skandalas), tai tampa konkurencingais veiksniais verslo ir vartotojų atžvilgiu visame pasaulyje.[77] XXI a. prasidėjus duomenų apsaugos teisės globalizacijai[78], ES savo nors ir griežtu reguliavimu pripažįstama technologijų reguliavimo lydere, veikiančia net gi tai, kaip kitos šalys reaguoja į didžiausių

[75] BERGGRUEN, N. *et al.* A wakeup call for Europe 2018, *Washington Post*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.washingtonpost.com/news/theworldpost/wp/2018/09/27/europe/>.
[76] Žr. pvz. 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final, p. 4 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.
[77] KUZIEMSKI, M. *et al*. AI Governance Post-GDPR: Lessons Learned and the Road Ahead, European University Institute, Policy brief, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cadmus.eui.eu/bitstream/handle/1814/64146/STG_PB_2019_07-EN.pdf?sequence=1&isAllowed=y>.
[78] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 47.

pasaulyje technologijų platformų galią ir įtaką.[79] Kokių esminių sprendimų imtasi DI ir duomenų reguliavime ES?

ES stiprina bendradarbiavimą dėl DI visoje Sąjungoje, kad padidintų savo konkurencingumą ir užtikrintų ES vertybėmis pagrįstą pasitikėjimą. Kadangi DI tapo strateginės svarbos sritimi ir pagrindiniu ekonomikos vystymosi varikliu, neatsiejamai veiksmų imasi ES institucijos nagrinėdamos socialinį, ekonominį, teisinį ir etinį DI poveikį visuomenei. Kintantys Europos DI standartai kuriami greta potencialiai konkuruosiančių standartų JAV ir Kinijoje (Baltojoje knygoje šios valstybės nurodomos kaip dabartiniai DI investicijų lyderiai). Ursula von der Leyen savo, kaip kandidatės į EK pirmininkės poziciją, darbotvarkėje Europai, dėstė, jog užtikrins, kad prioritetas būtų teikiamas investicijoms į DI tiek per daugiametę finansinę programą, tiek aktyviau naudojant viešojo ir privačiojo sektorių partnerystes.[80] Tačiau koks poveikis asmens duomenų reguliavimui?

Per pastaruosius kelerius metus pasirodė be galo daug regione išleistų su DI susijusių aktų, kaip antai DI strategija[81], Suderintas DI planas[82], komunikatas „Dirbtinis intelektas Europai“[83], DI ALEG Patikimo DI politikos ir investicijų rekomendacijos[84] ir dirbtinio intelekto apibrėžtis[85], Koordinuotas DI planas „Pagaminta Europoje“[86], Europos

[79] Žr. pvz. SATARIANO, A. *et al*. Europe, Overrun by Foreign Tech Giants, Wants to Grow Its Own, *the New York Times*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.nytimes.com/2020/02/19/business/europe-digital-economy.html>.

[80] VON DER LEYEN, U. *My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024*, p. 13 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf>.

[81] 2018 m. balandžio 25 d. Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Dirbtinis intelektas Europai, COM/2018/237 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/LT/COM-2018-237-F1-LT-MAIN-PART-1.PDF>.

[82] 2018 m. gruodžio 7 d. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions Coordinated Plan on Artificial Intelligence, COM/2018/795 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>.

[83] 2018 m. balandžio 25 d. Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Dirbtinis intelektas Europai, COM/2018/237 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/LT/COM-2018-237-F1-LT-MAIN-PART-1.PDF>.

[84] 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Policy and investment recommendations for trustworthy Artificial Intelligence [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>.

[85] 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Definition of AI: Main Capabilities and Disciplines [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

[86] 2018 m. gruodžio 7 d. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions Coordinated Plan on Artificial Intelligence, COM/2018/795 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>.

Parlamento rezoliucija su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų[87], Komunikatas dėl pasitikėjimo stiprinimo į žmogų orientuoto dirbtinio intelekto srityje[88], Bendradarbiavimo dirbtinio intelekto srityje deklaracija[89], Baltoji knyga ir kt. Be to, daugelis Europos šalių, tarp jų ir Lietuva[90], pagal reikalavimus parengė strategijas, kaip remti DI plėtrą ir išnaudoti jos teikiamą naudą savo šalims, jose aptartos su DI susijusios problemos, kylančios santykyje su moksliniais tyrimais, duomenų privatumu, užimtumu ir visuomenės švietimu. Ne viename iš pirma nurodytų ES ir šių nacionalinių dokumentų, skiriamas dėmesys ir DI poveikiui asmens privatumui bei asmens duomenų apsaugos teisei. Visgi, bendra tendencija tokia, jog šiuose skirtingų formų aktuose paprastai tik bendrai dėstomos su tuo susiję principinės ES nuostatos ar pasirenkamas strateginių tikslų dėstymas, retai svarstoma, kaip būsimi DI teisės aktai derėtų su ES duomenų apsaugos įstatymais ir juos papildytų[91], ar konkrečiai sprendžiami duomenų apsaugos klausimai.

Duomenų apsaugos reguliavimo šaknimis ES teisinėje bazėje išlieka ES pagridininių teisių chartijoje įtvirtintos teisė į privatų ir šeimos gyvenimą (7 str.) bei teisė į asmens duomenų apsaugą (8 str.). Panagrinėjus ES duomenų apsaugos sprendimų raidą detaliau, būtent technologijų proveržis XX-XXI a.[92] iškėlė poreikį spręsti technologijų raidos nenuspėjamumo problemą ir asmens duomenų apsaugos atžvilgiu. Kilo poreikis užtikrinti, kad įstatymai būtų tvarūs ir pakankamai universalaus pritaikomumo, todėl orientuojantis ne į kategoriškas normas, o daugiau principais grįstą reguliavimą, ES buvo vystoma duomenų apsauga. Pradedant Duomenų apsaugos direktyva, vienodinta nacionaliniu mastu valstybėse narėse savarankiškai besivysčiusi įstatymų leidyba, vėliau reguliavimas iš esmės plėtotas orientuojant į specifines duomenų apsaugos sritis, priimant

[87] 2017 m. vasario 16 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)) OL C 252, 2018 7 18 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017IP0051>.
[88] 2019 m. balandžio 8 d. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human Centric Artificial Intelligence, COM(2019) 168 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.
[89] 2018 m. balandžio 10 d. EU Member States Declaration of cooperation on Artificial Intelligence [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence>.
[90] 2019 m. kovo 8 d. Lietuvos Dirbtinio intelekto strategija [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://kurklt.lt/wp-content/uploads/2019/04/DI_strategija_LT_koreguota.pdf>.
[91] Žr. pvz. 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.
[92] Žr. pvz. United Nations Technology and innovation report 2018 p. 5 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://unctad.org/en/PublicationsLibrary/tir2018_en.pdf>.

ES institucijų duomenų apsaugos reglamentą[93], Direktyvą dėl privatumo ir elektroninių ryšių[94] (svarstomas privatumo ir elektroninių ryšių reglamento priėmimas[95]), Teisėsaugos direktyvą ir BDAR. Be to duomenų apsaugos teisės vystymui reikšmingai pasitarnavo 29 str. darbo grupė ir nuo BDAR įsteigta – EDAV leidžiant teisės aktų taikymo aiškinimo rekomendacijas, gaires ir kitus *soft law* šaltinius[96].

Visgi nors dauguma ES duomenų apsaugos teisės aktų vienaip ar kitaip atitinkamam kontekste ir apimtimi nebuvo niekaip atriboti nuo taikymo DI, išskirtinę reikšmę DI apdirbančio asmens duomenis reguliavimo kontekste įgijo būtent 2018 m. gegužės 25 d. ES įsigaliojęs BDAR. BDAR persvarstė ir suderino ES duomenų apsaugos sistemą, nustatydamas, kaip įprasta vertinti, griežčiausią pasaulyje duomenų apsaugos režimą. ES laikytina pasaulio lydere nustatant vartotojų duomenų privatumo standartus.[97] BDAR pasauliniu mastu buvo įvertintas kaip revoliucija duomenų apsaugos srityje. Kilo didelės diskusijos dėl to, ką įstatymas reiškia duomenims imlių technologijų ateičiai Europoje. Vienų tvirtinama, kad BDAR reikalavimai reiškia didžiųjų duomenų analizės Europoje pabaigą[98], kitų manoma, kad įstatymas leis didesniu mastu klestėti didiesiems duomenims[99]. Panašios diskusijos siautėjo ir dėl BDAR poveikio blokų grandinei (angl. blockchain)[100] bei aktualiausiam – DI. Visgi platesniai šio dokumento analizei skiriamos II-III šio magistro darbo dalys.

[93] 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, PE/31/2018/REV/1, OL L 295, 2018 11 21.

[94] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje, OL L 201, 31.7.2002.

[95] Pasiūlymas Europos Parlamento ir Tarybos Reglamentas dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB, COM/2017/010 final - 2017/03 (COD).

[96] žr. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_lt>.

[97] European Union Agency for Fundamental Rights Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf>.

[98] ZARSKY, T. Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646>.

[99] MAYER-SCHÖNBERGER, V. *et al*. Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation, *Columbia Science & Technology Law Review* Vol. XVII, 2016 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://informationaccountability.org/wp-content/uploads/SchonbergerPadova.pdf>.

[100] ARNOLD, A. Can Blockchain Help Brands Become GDPR Compliant? 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/#361b8fdf1203>.

1.2.2 Lietuvos priemonės dirbtinio intelekto ir duomenų apsaugos kontekste

Įsigaliojus BDAR, Asmens duomenų teisinės apsaugos įstatymo po BDAR reguliavimo apimtimi pakliuvusios nuostatos 2018 m. liepos 15 d. neteko galios[101]. Asmens duomenų apsaugos įstatyminis reguliavimas DI kontekste, kiek tai nebūtų sureguliuota BDAR, Lietuvos jurisdikcijoje nevystytas. Visgi Lietuvoje pastebėtini du svarbesni strateginiai daugiau orientacinio pobūdžio sprendimai sprendimai DI srityje: (i) „AI in the Nordic-Baltic Region“ tarptautinė deklaracija[102] bei (ii) Lietuvos dirbtinio intelekto strategija[103].

2018 m. Šiaurės ir Baltijos šalių ministrai pasirašė bendrą deklaraciją „AI in the Nordic-Baltic Region“. Kartu jie susitarė stiprinti bendradarbiavimą DI srityje, išsaugojant pirmaujančio Europos regiono pozicijas skaitmeninės plėtros srityje. Deklaracijoje nurodytos septynios pagrindinės sritys, kuriomis siekiama plėtoti ir skatinti DI naudojimą siekiant geriau tarnauti žmonėms. Kalbant apie privatumą, ketvirtojoje tikslinėje srityje sulygta dėl bendro siekio, kad infrastruktūra, techninė įranga, programinė įranga ir duomenys, kurie visi yra labai svarbūs DI naudojimui, būtų grindžiami standartais, leidžiančiais sąveikai, privatumui, saugumui, pasitikėjimui, tinkamam naudojimui ir perkeliamumui.

2018 m. Lietuvoje buvo žengti ir pirmieji žingsniai, siekiant reglamentuoti DI kūrimo ir panaudojimo principus nacionaliniu mastu. Ekonomikos ir inovacijų ministerija kartu su įvairių sričių privataus ir viešojo sektoriaus ekspertų grupe pradėjo diskusijas dėl DI technologijų įtakos, svarbos įvairiose gyvenimo srityse ir LR galimybių įgyvendinti ar dalyvauti įgyvendinant DI projektus. Galiausiai buvo parengtos strateginės įžvalgos, dėl esamos padėties šalyje DI srityje, pagrindiniai etiniai ir teisiniai klausimai DI kūrimo ir naudojimo srityse, įgūdžių ir kompetencijų, kurių reikia darbui su DI, didinimo galimybės ir būdai, DI mokslinių tyrimų ir ekspertinės plėtros augimo galimybės.[104] Rezultate 2018

[101] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas, *TAR*, 2018-07-11, Nr. 11733.
[102] 2018 m. gegužės 14 d. Nordic Council of Ministers AI in the Nordic-Baltic region [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.regeringen.se/49a602/globalassets/regeringen/dokument/naringsdepartementet/20180514_nmr_deklaration-slutlig-webb.pdf>.
[103] 2019 m. kovo 8 d. Lietuvos Dirbtinio intelekto strategija [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://kurklt.lt/wp-content/uploads/2019/04/DI_strategija_LT_koreguota.pdf>.
[104] Lietuvos Respublikos Vyriausybės 2019 m. gegužės 8 d. nutarimas Nr. 461 „Dėl 2019 metų Nacionalinės reformų darbotvarkės patvirtinimo“, *TAR*, 2019-05-14, Nr. 2019-07654.

m. EK komunikato dėl suderinto DI plano[105] pagrindu buvo parengta ir Lietuvos nacionalinė DI strategija. Nurodomas Lietuvos DI strategijos tikslas – remiantis esamais ištekliais, patirtimi ir potencialu, tapti regiono lydere, didinti Lietuvos konkurencingumą tarp ES šalių ir sėkmingai įsitraukti į pasaulinę DI ekosistemą.[106] Ataskaitoje pateikiamos esminės ekspertų grupės projekto išvados apie DI padėtį Lietuvoje, pateikiama DI apibrėžtis bei DI plėtros ir įdiegimo sąlygų Lietuvoje analizė. Konkrečiai duomenų apsaugos atžvilgiu vienas iš orientyrų strategijoje – atsakingas ir veiksmingas požiūris į duomenis. Lietuvos Vyriausybė, dėstoma, jog imasi iniciatyvų, kurių tikslas – sukurti atvirų duomenų ekosistemą viešajame sektoriuje, be to išdėstomos ir strateginės rekomendacijos: (i) sukurti stabilią ir DI palankią duomenų aplinką, pagrindinį dėmesį sutelkiant į viešąjį sektorių; (ii) užtikrinti, kad Lietuvos duomenys atitiktų tarptautinių standartų reikalavimus.

Visgi Lietuvos strategija visuomenėje dėl DI apibrėžties buvo sukritikuota dėl nekokybiškai ir atmestinai išverstų esminių technologinių sąvokų bei DI per ankstyvo personifikavimo (ar bent tokios dokumento teksto formuluotės)[107]. Tokia išreikšta pozicija pabrėžta, koks svarbus teisingas DI suvokimas, kad būtų galima kurti validžią teisinę erdvę ir sudaryti adekvačias galimybes tolimesniems šios technologijos tyrimams.

Taigi kalbant asmens duomenų apsaugos reguliavimą Lietuvos mastu, privalomo detalesnio, nei ankstesniame skirsnyje išdėstyto ES reguliavimo nėra. Kol kas pažanga DI apdirbančio asmens duomenis srityje apsiriboja išleista DI strategija bei pasirašyta tarpvyriausybine deklaracija.

---

[105] 2018 m. gruodžio 7 d. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions Coordinated Plan on Artificial Intelligence, COM/2018/795 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>.

[106] GAUBIENĖ, N. *Lietuvos dirbtinio intelekto strategija: ar teisingai suprantamas dirbtinis intelektas?* TeisėPro, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www.teise.pro/index.php/2019/08/26/n-gaubiene-lietuvos-dirbtinio-intelekto-strategija-ar-teisingai-suprantamas-dirbtinis-intelektas/>.

[107] GAUBIENĖ, N. *Lietuvos dirbtinio intelekto strategija: ar teisingai suprantamas dirbtinis intelektas?* TeisėPro, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www.teise.pro/index.php/2019/08/26/n-gaubiene-lietuvos-dirbtinio-intelekto-strategija-ar-teisingai-suprantamas-dirbtinis-intelektas/>.

1.2.3 Dirbtinio intelekto reguliavimo ES ir JAV palyginimas

XXI a. prasidėjus duomenų apsaugos teisės globalizacijai[108] ir DI pagrindu veikiančių produktų pasiūlai nepriklausomai nuo kilmės įprastai peržengiant ne tik atskirų valstybių tačiau ir žemynų ribas, svarbiu tampa sistemiškas reguliavimo pažangos vertinimas skirtingose jurisdikcijose. Tiek pagal 2019 m. statistiką kaip dominuojanti valstybė pagal finansuojamų startuolių skaičių, tiek ir bendrai nuosekli DI finansavimo lyderė pasaulyje yra JAV.[109] Visapusiškam priemonių reguliuoti duomenis apdirbantį DI nagrinėjimui ES reguliavimas palygintinas su vieno svarbiausių DI rinkos *žaidėjų* globaliu mastu – JAV – aktualiais įstatymų leidėjo sprendimais.

2019-iais JAV, nors federalinė politika išlieka, kaip įprasta vertinti, gana palanki technologijų ir verslo vystymui, visgi, pastebėtina įstatymų leidėjų reakcija į didėjantį visuomenės susirūpinimą dėl nevaržomos technologinės plėtros pavojų. Pasiūlyta keletas aukšto lygio įstatymo projektų, kuriuose aptariamas DI vaidmuo, brėžiami orientyrai kaip jis turėtų būti valdomas, pasirašytas JAV prezidento vykdomasis įsakas dėl Amerikos lyderystės DI srityje išsaugojimo, išleidžiantis aktą – Amerikos DI iniciatyva[110]. DI strategijos kontekste JAV bendrai prieita išvados, kad DI technologijai kaip saugikliai galėtų būti nustatomi techniniai standartai ir sertifikavimo procedūros atitikčiai užtikrinti ir priežiūrai vykdyti.

Vertinant situaciją konkrečiai iš duomenų apsaugos perspektyvos, atkreiptinas dėmesys, jog JAV išsamaus duomenų apsaugos reguliavimo ilgą laiką išvis nebuvo. Pirmosios pataisos, taip pat trečiosios, ketvirtosios, penktosios, dešimtosios ir keturioliktosios pataisų teisminis aiškinimas atliko svarbų vaidmenį nagrinėjant pagrindinius privatumo aspektus, tačiau tiesioginių nuorodų į privatumą arba duomenų apsaugą nei Konstitucijoje, nei pataisose nebuvo. Trūko ir išsamaus privatumo ir (arba) duomenų apsaugos reguliavimo federaliniu lygmeniu. Šiuo metu asmens duomenų tvarkymas federalinėse institucijose reglamentuojamas 1974 m. Privatumo įstatyme[111] ir

---

[108] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 47.

[109] MISHRA, S. *et al*. *Artificial Intelligence Index 2019 annual report*, Stanford Human Centered Artificial Intelligence, p. 90 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf>.

[110] Organisation for Economic Cooperation and Development. *AI policies and initiatives, Overview of AI national policy responses*, OECD Library [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/AtIiS72>.

[111] Privacy Act of 1974 5 U.S.C. § 552a As Amended [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cia.gov/library/readingroom/docs/pa.pdf>.

įvairiuose valstijų įstatymuose. Teigiama, jog privačiame sektoriuje privatumo ir duomenų apsaugos reguliavimo labai trūksta, asmenims paliekama savireguliacija.[112]

Visgi, nors ir griežtai neorientuojant į DI technologijas, pastaruoju metu pažymėtini keli pokyčiai duomenų privatumo srityje. Už Atlanto BDAR sustiprino vis didesnę paramą federaliniam duomenų apsaugos įstatymui. Diskusijos dėl duomenų apsaugos ir privatumo JAV tradiciškai vyko tarp (i) „valstybės nesikišimo“ (pranc. *laissez-faire*[113]) požiūrio į duomenų apsaugą ir privatumą šalininkų bei (ii) tų, kurie pritaria didžiųjų technologijų reguliavimui. Iš pradžių Prezidento administracijos atsakas į BDAR visiškai atitiko *laissez-faire* konceptą – prekybos sekretorius Wilburas Rossas teigė, kad Europos duomenų apsaugos sistema gali tapti prekybos kliūtimi.[114] Visgi vėliau bendrai pritarta teisės aktų, kuriais bus siekiama apsaugoti vartotojų privatumą internete, idėjai – Baltieji rūmai galiausiai pareiškė, kad, konsultuodamiesi su didžiosiomis technologijų kompanijomis, rengia vartotojų privatumo internete įstatymo projektą[115].

Greta federalinės valdžios dar nesimaterializavusių siekių, kelios valstijos jau pradėjo taikyti savo duomenų privatumo taisykles.[116] Išskirtinai pažymėtinas Kalifornijos atvejis – priimtas Kalifornijos vartotojų privatumo įstatymas[117], kurį daugelis prilygino „Amerikos BDAR“[118]. Nors Kalifornijos privatumo įstatymo projektas ne toks platus kaip BDAR, tikėtina, kad 2020 m. įsigaliojus iš esmės paveiks technologijų bendrovių duomenų rinkimą ir naudojimą.[119]:

---

[112] NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018, p. 286.

[113] Pažodžiui liet. *leiskite veikti*.

[114] NEIDIG, H. *Trump Commerce chief: EU data privacy law could hurt trade*, the Hill, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://thehill.com/policy/technology/389948-wilbur-ross-says-gdpr-could-hurt-trade>.

[115] SHEPARDSON, D. Trump administration working on consumer data privacy policy iš *Reuters*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK>.

[116] National Conference of State Legislatures *2019 Consumer Data Privacy Legislation*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx>.

[117] California Consumer Privacy Act of 2018, 1798.100 - 1798.199, Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375&showamends=false>.

[118] Zurkus, K. *Understanding California's Consumer Privacy Act: The 'American GDPR'*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://securityintelligence.com/understanding-californias-consumer-privacy-act-the-american-gdpr/>.

[119] LYON, H. M. *et al. 2019 Artificial Intelligence and Automated Systems Annual Legal Review*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.gibsondunn.com/wp-content/uploads/2020/02/2019-artificial-intelligence-and-automated-systems-annual-legal-review.pdf>.

Bendrai įvertinus aukščiau nurodyta, galimos tokios įžvalgos, jog (i) DI kontekste tiek ES tiek JAV leidžiami DI strategiją formuluojantys aktai; (ii) lyginant su ES pastarosiomis iniciatyvomis ir sprendimais asmens duomenis apdirbančio DI reguliavimo kontekste, JAV atveju daugiau koncentruojamasi į technologijų vystymo perspektyvas, bendrus DI strategijos klausimus nei į duomenų apsaugą stiprinančią teisėkūrą; (iii) laiko prasme gana akivaizdus ES aktualiai sugriežtinto duomenų apsaugos reguliavimo poveikis JAV – duomenų tvarkymo procedūrų reguliavimas palengva tampa ir JAV įstatymų leidėjo interesu.[120] Atskirų valstijų teisėkūra net gi vertinama kaip griežtumu gana panaši į BDAR reguliavimą. (iv) Visgi į duomenų apsaugos stiprinimą orientuotoje JAV įstatymų leidyboje, lyginant su ES, rezultatų kol kas pasiekta vienareikšmiškai mažiau, ir tik valstijų lygiu. Tokia teisėkūra ES atveju[121] pagal taikymo mastą ir suderinimo lygį prilygtų ES valstybių savireguliacijai duomenų apsaugos srityje dar iki BDAR pirmtakės – Duomenų apsaugos direktyvos įsigaliojimo.

[120] Tokie pokyčiai, be abejo, gali būti siejami ir su politinėmis aktualijomis, turint omenyje pvz. rinkėjų duomenų saugumo stiprinimą (po pasaulinio lygio *Cambridge Analytica* bylos), ir kitais faktoriais.
[121] Visiškai principine prasme, nelyginant formalumų.

2 BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS KAIP DIRBTINIO INTELEKTO REGULIAVIMO ŠALTINIS

Naujasis reglamentas priimtas kaip svarbiausia ES duomenų apsaugos teisės reformos dalis.[122] Koncepcija buvo grįsta reakcija į riziką, kad trečiosios kartos teisės aktai praras aktualumą ir efektyvumą.[123] Siekta ne tik pagrindinio duomenų apsaugos reguliavimo šaltinio formos keitimo (iš direktyvos į reglamentą), tačiau bandyta persvarstyti technologinių, socialinių ir ekonominių pokyčių poveikį duomenų apsaugos reguliavimui, kad būtų tinkamai užtikrinta duomenų subjektų teisių apsauga ir sudarytos sąlygos adekvačiai asmens duomenų kontrolei.

Prieš detalų reikšmingiausių BDAR DI taikytinų nuostatų vertinimą trečiojoje darbo dalyje, svarbu atsižvelgti į keletą bendrų aspektų ir BDAR taikymo DI prielaidų.

2.1 Asmens duomenų apibrėžimas

BDAR pagal materialinę taikymo sritį yra taikomas ne bet kokios informacijos, o asmens duomenų tvarkymui.[124] DI kontekste tai lemia BDAR taikymą tik tokiam DI, kuris apdirba asmens duomenis, kaip jie suprantami pagal BDAR: (i) bet kokia informacija (ii) apie (iii) fizinį asmenį, (iv) kurio asmens tapatybė yra nustatyta arba gali būti nustatyta.[125]

Asmens duomenų kontekste informacija pagal pobūdį apima visus teiginius apie asmenį – kad būtų laikoma duomenimis, ji neturi būti teisinga ar įrodyta.[126] Turinio prasme – tai bet kokia informacija – tiek kontaktiniai duomenys, socialinis elgesys, pomėgiais, genetiniai ir biometriniai duomenys ir kt.[127], neatsižvelgiant į subjekto padėtį ar pareigas. Informacija gali būti pateikiama bet kokiu formatu ir nesvarbu kokiu būdu – raštu, taip pat

[122] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 301.
[123] KISS, A. *et al*. Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation iš GUTWIRTH, S. et al. (eds.) *Reforming European Data Protection Law*, Springer, Netherlands [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/312775175_Evolution_or_Revolution_Steps_Forward_to_a_New_Generation_of_Data_Protection_Regulation>.
[124] BDAR, 2 str. 1 d.
[125] *Ibid*, 4 str. 1 d.
[126] 2007 m. birželio 20 d. ES 29 str. Darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 9 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf>.
[127] Pvz., per piešimo programą kompiuteryje vaiko pieštas šeimos portretas, siekiant atlikti psichiatrinį vertinimą kaip vaikas jaučiasi dėl skirtingų savo šeimos narių, gali būti laikomas asmens duomenimis, jei piešinyje atskleidžiama informacija apie vaiką (jo psichinę sveikatą) ir tėvų elgesį.

kompiuterio atmintyje, debesyje ar bet kokioje laikmenoje. DI kontekste tai paprasčiausiai galima atspindėti per asmens duomenis surenkamus tiek iš fizinių asmenų veiklos viešojoje skaitmeninėje erdvėje (pvz. „*patinka*“ paspaudimų „Facebook“), tiek pačių subjektų pateikiamos informacijos apie save pvz. paskyroje „Linkedin“, nesprendžiant jos pagrįstumo.

Informacija laikytina asmens duomenimis turi turėti sąsają su asmeniu, būti apie tą asmenį[128]. Duomenys yra susiję su asmeniu, jeigu jie nurodo asmens tapatybę, ypatybes ar elgesį arba jei tokia informacija naudojama siekiant nustatyti kaip elgiamasi su tuo asmeniu arba kaip jis vertinamas, arba daryti jam poveikį.[129] Informacija gali būti sietina per tiesioginį santykį su asmeniu ir netiesioginį, t. y. pirma sietina su objektais, tačiau tie objektai priklauso asmeniui arba asmeniui daro tam tikrą poveikį, iš kurio vėl gi galima identifikuoti sąsają su specifiniu asmeniu.[130] Taigi ne tik DI renkama netiesiogiai su asmeniu susijusi informacija gali patekti po BDAR saugomų asmens duomenų apimtimi, tačiau ir pvz. automobilio priklausančio fiziniam asmeniui numeriai ir kt.

BDAR, kaip ir bendrai įprasta duomenų apsaugos teisėje, saugo būtent fizinių asmenų duomenis. Pagal fizinio asmens sampratą BDAR, reguliavimas netaikomas (i) duomenų, susijusių su juridiniais asmenimis apsaugai, (ii) mirusiems asmenims (pagal bendrą taisyklę)[131]. Todėl pvz. DI apdirbant bendrovių duomenis ir iš to vedant atitinkamas prognozes ir analizės rezultatus atitiktis BDAR – neprivaloma, tai reguliuoja kiti teisės aktai.

Galiausiai svarbus aspektas tai, jog BDAR netaikomas (i) anonimiškai informacijai, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba (ii) anonimizuotiems asmens duomenims, kad duomenų subjekto tapatybė negalėtų būti nustatyta.[132] Sprendžiant, ar galima nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visas priemones, kurias asmens tapatybei tiesiogiai ar netiesiogiai nustatyti, pagrįstai tikėtina, galėtų naudoti duomenų valdytojas. Tokiu atveju reikia atsižvelgti į visus

[128] 2007 m. birželio 20 d. ES 29 str. Darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 9 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf>.
[129] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 93.
[130] 2007 m. birželio 20 d. ES 29 str. Darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 9 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf>.
[131] Šiuo atveju fizinio asmens sąvoka aiškintina pagal civilinės teisės nuostatas – Lietuvos Respublikos civilinio kodekso, Valstybės žinios, 2000-09-06, Nr. 74-2262, 2.1 str. ir 2.2 str. 1 d.
[132] BDAR 26 konst. d. p.

objektyvius veiksnius, turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą.[133] Naudojant DI, tai reiškia, jog BDAR netaikytinas tik objektyviai anonimizuotai informacijai, kurios net ir turint omenyje DI potencialą DI negalėtų niekaip susieti su konkrečiu asmeniu. Visgi dėl visiško nesusiejamumo susidurtina su tam tikra problematika minėta darbo 1.1.3 dalyje – DI pasitelkiant profiliavimui, analizuojant didelį kiekį net ir anonimizuotų duomenų, specifiniai duomenys profiliuojant pagal elgesio tendencingumą, informacijos būdingumą gali pagal sukuriamą anonimiško vartotojo profilį tapti prisietini prie konkretaus asmens atgaliniu būdu. Šiuo atveju galima laikyti, jog duomenų apdirbimo procese informacija tampa duomenimis neapibrėžtu momentu.

Taigi sprendžiant, ar DI apdirbant duomenis yra taikytinas BDAR, yra itin svarbu įvertinti materialinį BDAR taikymo aspektą – ar duomenys patenka po BDAR įvardintų asmens duomenų apibrėžtimi.

2.2 Teritorinio taikymo apimtis

Aktas, kuriuo siekta suderinti duomenų apsaugos teisės aktus ES valstybėse narėse ir sugriežtinti duomenų apsaugos taisykles tapo duomenų apsaugos reguliavimo pavyzdžiu visame pasaulyje. Visgi ne tik kaip atspirties taškas įstatymų leidėjams ir mokslininkams, tačiau ir realaus taikymo prasme BDAR yra aktualus globaliu mastu.

Pagal teritorinio taikymo taisykles reglamentas gali būti tiesiogiai taikomas duomenų tvarkytojams nei formaliąja (buveinė), nei materialiąja (buvimo lokacija) prasme nesantiems ES. Pagal bendrą taisyklę galimi trys alternatyvūs atvejai, kuomet DI apdirbant duomenis galėtų būti taikomas BDAR: (I) kai duomenų tvarkytojo ir valdytojo buveinė ES, nepriklausomai nuo to, kur DI iš esmės atlieka duomenų tvarkymą[134]; (II) kai duomenų valdytojas įsisteigęs valstybėje, kurioje taikytina ES teisė[135] ir (III) kai veikla susijusi su (i) prekių / paslaugų siūlymu ES esantiems duomenų subjektams, neatsižvelgiant į tai, ar už tai reikia atsiskaityti, arba (ii) duomenų subjekto elgesio ES stebėsenos veikla[136]. Nors pirmi du atvejai gana aiškios formuluotės, trečiojo, kuris itin aktualus duomenis apdirbant globaliu mastu įvairiose šalyse esantiems tvarkytojams taikymas nėra toks konkretus.

[133] BDAR 26 konst. d. p.
[134] *Ibid.* 3 str. 1 d.
[135] *Ibid.* 3 str. 3 d.
[136] *Ibid.* 3 str. 2 d.

Siekiant aiškumo, EDAV priėmė gaires dėl BDAR teritorinio taikymo[137], kuriose nurodyta, kad siekiant nustatyti, ar tvarkymo veiklai taikytinas šis punktas, būtina išnagrinėti, ar duomenų tvarkytojo tvarkymo veikla „yra susijusi“ su duomenų valdytojo tiksline veikla. Jei duomenų valdytojo vykdoma tvarkymo veikla susijusi su prekių ar paslaugų teikimu arba su asmenų elgesio ES stebėsena (nukreipimas), tai ir bet kuriam duomenų tvarkytojui, kuriam pavesta duomenų valdytojo vardu vykdyti duomenų tvarkymo veiklą, bus taikomas BDAR 3 str. 2 d.[138]. EDAV siūlo sutelkti dėmesį į duomenų tvarkytojo vykdomos apdorojimo veiklos ir duomenų valdytojo vykdomos tikslinės veiklos ryšį. Jei duomenų tvarkytojo vykdoma duomenų tvarkymo veikla, valdytojo nurodymu, yra susijusi su prekių ar paslaugų teikimu duomenų subjektams esantiems ES, duomenų tvarkytojui, kuris nėra įsisteigęs ES, bus taikomas BDAR.

BDAR taikymo apimtis yra viena reikšmingiausių BDAR reguliavimo ypatybių, dėl kurios visiems nustatytus taikymo kriterijus atitinkantiems ES ir ne ES subjektams yra privaloma užtikrinti pasitelkiamo asmens duomenis apdirbančio DI atitiktį ES sukurtai BDAR taisyklių visumai. Turint omenyje stambiausių pasaulinėje rinkoje veikiančių korporacijų DI taikymą išmaniuosiuose įrenginiuose, programėlėse ar interneto puslapiuose, skirtuose vartotojams visame pasaulyje, ES ribas peržengianti BDAR taikymo apimtis gali daryti įtaką į pasaulinę rinką orientuotų DI sistemų kūrimui. Tai gali būti pagrindas jau kūrimo etape DI procesų derinimui prie BDAR reguliavimo siekiant DI sistemų visapusiško pritaikomumo tiek ES, tiek visame pasaulyje.

2.3 Santykis tarp duomenų valdytojo, duomenų tvarkytojo ir dirbtinio intelekto

Visapusiam BDAR taikymo DI vertinimui svarbu išskirti, kam tiksliai kyla duomenų apsaugos reikalavimų užtikrinimo pareigos ir ypač atsakomybė už duomenų apsaugos pažeidimus. Šiuo atveju BDAR skiriami dviejų tipų subjektai – duomenų valdytojai ir duomenų tvarkytojai.

---

[137] 2019 m. lapkričio 12 d. European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf>.

[138] „*Šis reglamentas taikomas asmens duomenų tvarkymui, kai Sąjungoje esančių duomenų subjektų asmens duomenis tvarko Sąjungoje neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas ir duomenų tvarkymo veikla yra susijusi su: a) prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje, nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti; arba b) elgesio, kai jie veikia Sąjungoje, stebėsena.*“

Duomenų valdytojas – kiekvienas asmuo ar subjektas, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones[139]. Duomenų valdytojui būdingas teisinis subjektiškumas, t. y. pvz. juo laikytina ne bendrovėje dirbantis asmuo, o pati bendrovė. Pareiga įgyvendinti visus nustatytus reikalavimus, sugebėti įrodyti, kad jų laikomasi[140] ir galutinė atsakomybė dėl DI atitikties reguliavimui tenka būtent duomenų valdytojui. Tuo tarpu duomenų tvarkytojas yra (i) nuo duomenų valdytojo nepriklausomas, savarankiškas fizinis ar juridinis asmuo, (ii) tvarkantis duomenis duomenų valdytojo vardu[141].

Esminiai skirtumai tarp duomenų valdytojo ir duomenų tvarkytojo yra tai, jog (i) duomenų tvarkytojas yra nesavarankiškas tvarkant duomenis ir pagal bendrą taisyklę juos tvarko tik pagal duomenų valdytojo dokumentuose įformintus nurodymus[142]; (ii) pagrindinė atsakomybė už duomenų apsaugos pažeidimus taikoma duomenų valdytojui; (iii) duomenų tvarkytojo pareigos yra ribotos ir kyla tik konkrečiai numatytais BDAR atvejais[143].

Visgi pažymėtina su tuo susijusi problematika DI kontekste. Tam tikromis aplinkybėmis atskirti duomenų valdytojus ir duomenų tvarkytojus gali būti gana paprasta. Pvz., jei organizacija nusprendžia saugoti savo klientų duomenis debesyje, debesijos paslaugų teikėjas gali būti duomenų tvarkytoju, nes jis tiesiog veikia pirminės organizacijos vardu ir neapibrėžia apdorojimo tikslų. Tačiau kai asmens duomenys tvarkomi didžiųjų duomenų, DI ir mašininio mokymosi kontekste, gali būti sunkiau atskirti duomenų valdytojus ir duomenų tvarkytojus. Taip yra todėl, kad paprastai didžiųjų duomenų analizė yra susijusi su koreliacijų paieška, prognozių sudarymu ir pagalba priimant sprendimus. Visa tai nubrėžia ribas tarp to, kas iš tikrųjų nustato apdorojimo tikslus ir būdus, kai organizacija nusprendžia analitiką perduoti kitai bendrovei, pvz., tai, kuri specializuojasi DI. Todėl perduodant didelės apimties duomenų analizę kitoms bendrovėms, yra svarbu įvertinti, kur iš tikrųjų yra asmens duomenų tvarkymo kontrolė – tai daro esminę įtaką atitikčiai ir atsakomybei. Sutartyje tarp duomenų valdytojo ir duomenų tvarkytojo turi būti aiškios instrukcijos, kaip šiuos duomenis galima naudoti ir kokie konkretūs jų tvarkymo tikslai. Visgi, sutarties sudarymas *per se* nereiškia, kad duomenų analizę atliekanti

[139] BDAR 4 str. 7 d.
[140] *Ibid*. 5 str. 2 d.
[141] 2010 m. vasario 16 d. ES 29 str. darbo grupės Nuomnė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP 169, p. 24 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.
[142] Išimtys numatytos BDAR 28 str. 3 d. a p.
[143] J. Zaleskis skiria 6 duomenų tvarkytojo pareigas, nustatytas: (i) BDAR 28 str. 3 d., 29 str.; (ii) 32 str. 1 d., (iii) 37 str. 1 d. (iv) 30 str. 2 d., (v) 31 str. ir (vi) V BDAR sk. Žr. ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 103.

bendrovė yra duomenų tvarkytoja. Jei ši bendrovė turi pakankamai laisvės pasinaudoti savo patirtimi ir nuspręsti, kokius duomenis rinkti ir kaip taikyti analizės metodus, tikėtina, kad ji taip pat bus duomenų valdytoja.[144]

Vis dėlto, viena duomenų valdytojo ir tvarkytojo kategorijų skirties aspektu yra aišku, jog abu BDAR apibrėžimai[145] yra taikytini tik fiziniams arba juridiniams asmenims, valdžios institucijoms, agentūroms ar kitoms įstaigoms, kas reiškia, jog pats DI pagal aktualų reguliavimą neturėtų būti laikomas nei duomenų valdytoju, nei tvarkytoju, verčiau, duomenų valdytojo ar tvarkytojo pasitelkiama priemone. BDAR ribose dar negalime kalbėti apie konkrečias teisines pareigas, priskirtinas pačiam DI. Šiame darbe analizuojant BDAR taikymą DI laikytina, jog iš teisinės pusės kylančių pareigų atžvilgiu referuojama į BDAR subjektą, pasitelkiantį DI.

2.4 Pritaikomumas ilgalaikėje perspektyvoje

Galima būtų kvestionuoti, ar BDAR nėra vien kilnių tikslų deklaracija ir tik dar vienas reguliacinis tekstas, kurio „tvarumą“ galima ginčyti jau pradėjus jį įgyvendinti. Visgi BDAR nėra terminuoto galiojimo aktas, priimtas su perspektyva susidūrus su technologiniais pokyčiais, su laiku, jį pakeisti kitu aktu. Reguliavimo aktualumo ir pakankamumo ateityje klausimui spręsti autorės nuomone esmingai pasitarnauja pora įstatymo leidėjo įdiegtų BDAR saugiklių.

Pirma, nors kuriant duomenų apsaugos reguliavimo strategiją buvo atsižvelgta į skaitmeninės aplinkos pažangą ir sudėtingumą, BDAR formuluote Europos teisės aktų leidėjai aiškiai laikosi technologinio neutralumo principo[146], dar vadinamo nuo technologijų nepriklausoma teisėkūra.[147] Technologinis teisės neutralumas reikalauja, kad

[144] Pvz., straipsnyje dėl „Royal Free London NHS Foundation Trust“ duomenų perdavimo „Google DeepMind“ J. Powles teigta, jog, „DeepMind“ iš tikrųjų yra bendras duomenų valdytojas, o ne duomenų tvarkytojas [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://link.springer.com/article/10.1007/s12553-018-0226-6>. Tai atitinka ir ESTT praktiką, kur spręsta, jog ir Facebook ir Facebook gerbėjų tinklalapio administratorius turėtų būti laikomi duomenų valdytojais, žr. Europos Sąjungos Teisingumo Teismas. *2018 m. birželio 5 d. sprendimas byloje C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein prieš Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388.*

[145] BDAR 4 str. 7-8 d.

[146] BDAR 15 konst. d. nurodyta, kad fizinių asmenų apsauga turėtų būti technologiškai neutrali ir neturėtų priklausyti nuo naudojamų metodų.

[147] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, žr. p. 24-28 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

reguliavimas sukeltų tokį patį poveikį, neatsižvelgiant į technologinę aplinką, kurioje jis taikomas.[148] Dėl to bendrieji BDAR principai ir reikalavimai formuluoti taip, kad turėtų būti pakankamai lankstūs nuolatinei adaptacijai pritaikymui naujiems naudojimo atvejams, nenumatytiems BDAR sukūrimo metu. Visgi nors BDAR nėra konkrečiai skirtas DI, dabartinis DI modelis tiesiogiai patenka į BDAR taikymo sritį.[149]

Antra vertus, teisės akto aktualumui ir tvarumui ilgalaikėje perspektyvoje užtikrinti pasitelktas ir reglamento pakartotinės peržiūros įtvirtinimas. 97 str. numatyta EK kompetencija pirmąsyk 2020 m. gegužės 25 d. ir kas ketverius metus po to teikti ataskaitą Europos Parlamentui ir Tarybai. Prireikus EK pateikia atitinkamus pasiūlymus, kaip iš dalies pakeisti Reglamentą, visų pirma atsižvelgiant į informacinių technologijų raidą ir į informacinės visuomenės pažangą.

Iš esmės BDAR taisyklės ir principai ir yra pakankamai lanksčiai apibrėžti, kad apimtų būsimus technologinius pokyčius ir suteiktų ilgalaikę apsaugą. Visgi iš to neabejotinai kyla klausimų, kaip tiksliai interpretuoti kai kuriuos iš BDAR reikalavimų atsižvelgiant į technologijas, ir kokiu mastu BDAR yra tinkama teisinė priemonė sprendžiant technologijų poveikį individams. Negalima ignoruoti rizikos, kad kai kurioms sąvokoms ir koncepcijoms būdingi neaiškumai technologiniam pritaikomumui ilgainiui gali lemti didelius teisės aiškinimo skirtumus, taigi ir teisinį netikrumą.[150] Šiai problematikai spręsti išlaikant aptakų BDAR reguliavimą, vertintina, jog svarbų vaidmenį atlieka EDAV ir EK iniciatyva leidžiami komunikatai ir kitos formos aktai kuriais siekiama užpildyti BDAR spragas ir neaiškumus.

2.5 Interesų balansas reguliavime

Pasaulio mokslininkų reakcija į BDAR sukurtą reguliavimą yra skirtinga – priešpastatomi poreikiai užtikrinti tinkamą terpę inovacijoms *versus* fizinių asmenų duomenų apsaugos stiprinimą ketvirtosios pramonės revoliucijos kontekste. Saviems interesams pagrįsti –

[148] HILDEBRANDT, M. Data protection by design and technology neutral law, *Computer Law & Security Review* Volume 29, Issue 5, 2013, p. 510. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://works.bepress.com/mireille_hildebrandt/62/>.
[149] JACOBS, S. *et al*. *Data Privacy: Al and the GDPR*, Norton Rose Fulbright, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.insidetechlaw.com/blog/data-privacy-ai-and-the-gdpr>.
[150] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, žr. p. 24-28 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

žymus pasaulio mokslininkų indėlis dedamas į detalią pačios įstatymo raidės analizę – konkrečių nuostatų aiškumą, pakankamumą ir praktinį BDAR pritaikomumą.

Menkiausia užuomina apie reguliavimą paprastai išprovokuoja privataus verslo interesų, ypač technologijų pramonės (ir jų gerai apmokamų lobistų), pasipriešinimą, visapusišką kritiką, jog vienareikšmiškai reguliavimas stabdo inovacijas, pasiduodant fikcijai, pagal kurią inovacijos bet kuriuo atveju laikomos socialinio gėrio sinonimu[151]. „*Šiuo metu matome savotišką Laukinių Vakarų situaciją su DI reguliavimu. Mastas, kuriuo bendrovės diegia DI technologijas, neatitinka aiškių algoritmų reguliavimo gairių ir nepadeda tyrėjams išvengti duomenų rinkinių šališkumo problemų. Turime pasisakyti už geresnę kontrolės ir pusiausvyros sistemą, kad patikrintume DI šališkumą ir teisingumą, ir padėtume įmonėms nustatyti, ar tam tikri naudojimo atvejai šiuo metu yra tinkami šiai technologijai*.“[152] – Timnit Gebru, „Google AI“ tyrimų mokslininkė.

Reguliavimas tam tikra prasme tikrai apsunkina inovacijas – ypač kritikuojamas BDAR reikalavimas užtikrinti teisėtumą, skaidrumą ir atskaitomybę, tikslų ribojimą ir duomenų mažinimą. Be abejo, neigiamai iš verslo pusės vertinama ir galimybė skirti dideles baudas. Atkreiptinas dėmesys į tai, jog kai kurie iš šių aspektų net gi nėra nauji lyginant su ankstesniu Duomenų apsaugos direktyvos reguliavimu, visgi, visuomenės susidomėjimas duomenų apsauga ir išplėstas ES duomenų apsaugos taisyklių teritorinis taikymas davė peno pamąstymams dėl bet kokio galimo reguliavimo poveikio tiek retrospektyviai, tiek BDAR naujovių atžvilgiu.

Randasi ir tų, kurie kaip tik giria BDAR sulyg naujovių grąžinimu į socialinę kontrolę. Be to įžvelgiamos naudos ryšium su kibernetinio saugumo stiprinimu, duomenų apsaugos standartizacija, reputacijos išlaikymu, vartotojams sekant paskui atsakingai duomenis tvarkantį verslą.[153] Istoriniai duomenys rodo, kad tinkamai parengtas ir griežtas reguliavimas taip pat gali skatinti inovacijas įvairiomis kryptimis[154] – tokiu būdu pateikiamos aiškesnės instrukcijos inžinieriams ar kūrėjams, kurie norėtų kurti vartotojams patogius produktus.

---

[151] YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019.
[152] JOHNSON, N. *How Businesses Can Counter Bias in AI*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.salesforce.com/company/news-press/stories/2018/9/091718-e/>.
[153] TDS, *The Positive and Negative Implications of GDPR* [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr>.
[154] HART, D. M. *When Does Environmental Regulation Stimulate Technological Innovation? Information Technology & Innovation Foundation Report*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www2.itif.org/2018-environmental-regulation-innovation.pdf>.

Iš kitos perspektyvos pastebėtina, kad nuo BDAR įsigaliojimo, nors ir griežta, privatumo sistema yra net gi neproporcingai naudinga didelėms technologijų bendrovėms. Tokie rinkos žaidėjai kaip „Facebook“ ar „Google“, bet kuriuo atveju turi pakankamai išteklių ne tik laikytis tokių įstatymų, bet ir yra užtikrinti bet kuriuo atveju galėti atsistatyti po galimų sankcijų, lyginant su startuoliais ar mažesnėmis kompanijomis.[155]

Taigi iš vienos pusės dėl kiekvieno reglamento kai kurie veiksmai tampa nepriimtini – tai yra „tramdančioji“ valdymo pusė. Tačiau tampa aišku, kad toks reguliavimas kartu su kitomis inovacijas skatinančiomis pastangomis, vienaip ar kitaip yra svarus indėlis į duomenų apsaugos atžvilgiu atsakingą ir tvarų technologijų plėtros modelį.

***

Toliau darbe tiriama ar ir kaip konkrečios BDAR nuostatos taikytinos DI ir su kokia problematika susiduriama. Tam pasitelktinas konkrečių BDAR principų ir duomenų subjektams suteiktų teisių vertinimas apsiribojant labiausiai duomenų tvarkymo, atliekamo pasitelkiant DI, procesus veikiančiomis kategorijomis.

[155] LASKAI, L. *Year in Review: The Year of Data Protection*, Council on Foreign Relations, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cfr.org/blog/year-review-year-data-protection>.

3 BENDROJO DUOMENŲ APSAUGOS REGLAMENTO NUOSTATŲ TAIKYMAS DIRBTINIAM INTELEKTUI

Siekiant užtikrinti, kad į privatumo interesus būtų tinkamai atsižvelgta visame DI sistemų gyvavimo cikle, reikalingas *ex ante* ir *ex post* DI reguliavimo iššūkius apsprendžiantis duomenų apsaugos reguliavimas. Darbo tikslui pasiekti atitinkamo įverčio reikalauja konkrečios BDAR įtvirtintos nuostatos, jų pritaikomumas ir poveikis DI. Tam pasitelktina esminių DI kūrimui, procesų palaikymui ir organizavimui įtaką darančių principų ir iš įtvirtintų duomenų subjektų teisių DI kūrėjams ir DI pasitelkiantiesiems duomenų valdytojams kylančių pareigų analizė. Nors ir netiesiogiai orientuojant į DI (išlaikant technologinį neutralumą), BDAR turinyje išskirtinę reikšmę DI reguliavimui, autorės nuomone, įgyja įtvirtintos pritaikytosios ir standartizuotosios duomenų apsaugos principo, kaip tiek *ex ante*, tiek *ex post* DI formalių valdymo procesų atitikties duomenų apsaugos reikalavimams užtikrinimo principas, ir automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą, draudimas, kaip daugiau *ex post* DI duomenų apdirbimo procesų reguliavimo priemonė. Todėl, siekiant nuoseklaus bei konstruktyvaus BDAR taikymo DI vertinimo, darbe analizuotina DI reguliavimui reikšmingiausių BDAR principų ir duomenų subjektų teisių turinys ir taikymas DI, ypatingą dėmesį skiriant pritaikytosios ir standartizuotosios duomenų apsaugos principui bei autonominio automatizuoto atskirų sprendimų priėmimo reguliavimui.

3.1 Principai

BDAR nustatyti pagrindiniai asmens duomenų apsaugos principai. Teisės doktrinoje pripažįstama, kad neatsižvelgiant į technologinius pokyčius per kelis dešimtmečius nepasikeitę pagrindiniai duomenų apsaugos teisės principai išlieka efektyviu pasaulinių informacinių sistemų reguliavimo pagrindas.[156] Kai kurie jų – išsiskiria poveikiu DI technologijų kūrimui bei taikymui, su tikslu tvarkyti asmens duomenis. BDAR principų taikymo DI analizei darbo autorės pasirinkimu nagrinėtina (i) teisėtumo, sąžiningumo ir skaidrumo principo[157], (ii) duomenų tvarkymo tikslo apribojimo principo[158], (iii) duomenų

[156] KIRBY, M. The history, achievement and future of the 1980 OECD guidelines on privacy, *International Data Privacy Law*, Volume 1, Issue 1, 2010 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://academic.oup.com/idpl/article/1/1/6/759637>.
[157] BDAR 5 str. 1 d. a p.
[158] *Ibid*. 5 str. 1 d. b p.

mažinimo principo[159] ir (iv) pritaikytosios ir standartizuotosios duomenų apsaugos principo[160] turinys ir reikšmė.

3.1.1 Teisėtumo, sąžiningumo ir skaidrumo principas

Remiantis BDAR asmens duomenys duomenų subjekto atžvilgiu turi būti tvarkomi teisėtai, sąžiningai ir skaidriai.[161] Galima sakyti, jog iš esmės visas duomenų apsaugos teisės reguliavimas ir detalizuoja šį principą. Tai svarbiausias, plačiausios apimties ir abstrakčiausias duomenų apsaugos teisės principas.[162] BDAR 5 str. 2 d. suponuoja duomenų valdytojui pareigą ne tik imtis visų priemonių duomenų tvarkymo teisėtumui užtikrinti, tačiau ir sugebėti įrodyti, kad jo laikomasi (atskaitomybė). Konkretaus poveikio DI vertinimo tikslais, principo sudedamųjų – teisėtumo, sąžiningumo ir skaidrumo – kaip atskirų duomenų apsaugos teisės principų koncepcijos toliau nagrinėtinos atskirai.

3.1.1.1 Teisėtumas

Teisėtumo principas reiškia, jog duomenų tvarkymas turi būti legitimus visų duomenų apsaugos norminių teisės šaltinių atžvilgiu – atitikti ne tik BDAR, tačiau ir kitus tarptautinės ir nacionalinės teisės aktus. Pirmiausia, teisėtam asmens duomenų tvarkymui BDAR numato šešis galimus pagrindus.[163] Visgi, tai tik viena iš daugelio duomenų apsaugos vykdymo sąlygų,[164] ir pagal teisėtumo principą, duomenų tvarkymui visame duomenų apsaugos šaltinių kontekste, kiekvienu atveju duomenų valdytojas – be teisinio pagrindo buvimo vertinimo – kartu turi atsižvelgti ir į duomenų apsaugos teisės šaltinių tikslus, dvasią bei sistemą, ryšium su sąžiningumo principu nepiktnaudžiauti įstatymo *raide*. Teisėtumo reikalavimas, kaip ir kiti BDAR pagrindiniai principai, yra neatsiejamas pagrindas kitų BDAR duomenų tvarkymo nuostatų taikymui.

DI kontekste teisėtumo principo įgyvendinimas akivaizdžiai atsiskleidžia per teisę duoti sutikimą. Kadangi šiuo aspektu susiduriama su tam tikra problematika, ši duomenų

[159] BDAR 5 str. 1 d. c p.
[160] *Ibid*. 25 str.
[161] *Ibid*. 5 str. 1 d. a p.
[162] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 113.
[163] BDAR 6 str. 1 d.
[164] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 114.

subjekto teisė, autorės pasirinkimu ir atsižvelgiant į literatūroje pastebimą praktiką[165], nagrinėtina kartu su teisėtumo principu.

Nors BDAR nurodytos kelios asmeninės informacijos tvarkymo teisėtumo priemonės, pagrindinis būdas teisėtai tvarkyti vartotojų asmeninius duomenis yra aiškus sutikimas vienu ar keliais konkrečiais tikslais.[166] Šiuo atveju sutikimas yra bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys[167] – pvz. pažymint langelį interneto svetainėje, pasirenkant informacinės visuomenės paslaugų techninius parametrus arba kitu pareiškimu arba poelgiu, iš kurio aiškiai matyti tame kontekste, kad sutinkama su siūlomu asmens duomenų tvarkymu[168]. Tyla, iš anksto pažymėti langeliai arba neveikimas – neturėtų būti laikomi sutikimu. Duomenų valdytojas privalo galėti įrodyti, kad duomenų subjektas, be kitų sąlygų, nedviprasmiškai ir laisvai sutiko.[169]

Specifiškai reguliuojamas vaikų sutikimo davimas – pagal BDAR vaikas iki 16 m. arba pagal atskirų valstybių narių įstatymus iki 13 m. negali pats duoti sutikimo.[170] Visgi duomenų valdytojas gali sušvelninti savo atsakomybę imdamasis „pagrįstų pastangų“, siekiant patikrinti, ar yra tėvų sutikimas ar leidimas, tačiau imantis šių pastangų turi būti atsižvelgiama į turimas technologijas.[171] Problematika šiuo aspektu slypi tame, jog BDAR neapibrėžia nei „pagrįstų pastangų“, nei „turimų technologijų“ vertinimo kategorijų. Tai, vertintina, jog sustiprina duomenų valdytojų ir duomenų tvarkytojų priežiūros poreikį, kalbant apie vaikų teisių apsaugą iš viešojo intereso pusės. Lygiai taip suponuoja ir tam tikrą teisinį netikrumą iš technologijų kūrėjų pusės – projektuojant apie asmenis autonomiškai renkančius duomenis DI.

---

[165] Žr. Pvz. MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

[166] BDAR 6-7 str.

[167] *Ibid*. 4 str. 11 p.

[168] *Ibid*. 32 konst. d. p.

[169] *Ibid* 7 str. Pažymėtina, jog teisės duoti sutikimą aiškinimo tikslais yra priimta 2018 m. balandžio 4 d. Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>.

[170] 2018 m. balandžio 4 d. Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>. 8 str. 1 d.

[171] 2018 m. balandžio 4 d. Article 29 Working Party Guidelines on consent under Regulation 2016/679, WP259 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51030>. 8 str. 2 d.

Bendra prasme, informacijos privatumo supratimas lemia individų gebėjimą racionaliai pasirinkti, kokią informaciją apie juos turės kiti ir kas su tuo bus daroma. Tačiau dėl DI sudėtingumo duomenų tvarkymo techniniai procesai gali būti neaiškūs duomenų subjektams, todėl objektyvus, sąmoningas sutikimas gali būti net neįmanomas. Šiuo atveju atsiskleidžia akivaizdus sutikimo, kaip teisėtumo pagrindo ryšys su skaidrumu, kaip to paties principo sudedamąja. Visgi, giliojo mokymosi metodai gali kelti problemų skaidrumui, nes pateikti paaiškinimą, kaip DI daromos išvados, kartais gali būti sunku net pradinių algoritmų kūrėjams, jau nekalbant apie vidutinį asmenį. O nesant galimybės subjektų tinkamai informuoti, tiesiogiai susidurtina su sunkumais tiek užtikrinant skaidrumą DI veikloje, tiek gaunant sutikimą. Atliekama nemažai mokslinių tyrimų dėl „privatumo paradokso“ atsiradimo, kai žmonės reiškia susirūpinimą savo privatumu, tačiau praktiškai ir toliau noriai prisideda prie savo informacijos dalijimosi per naudojamas sistemas ir technologijas.[172] Praktiškai, net ir sritį išmanantys asmenys dažnai neturi kito pasirinkimo, kaip tik sudaryti „nesąmoningą sutartį“, kad galėtų leisti naudotis jų duomenimis,[173] tolimesniems veiksmams atlikti. Leidimas dažnai duodamas asmeniui mąstant, jog tiesiog nėra kitos išeities. Vertinama, jog dėl naudojamų sistemų sudėtingumo ir didėjančios duomenų rinkimo metodų įvairovės paprastas teigiamas arba neigiamas atsakymas į sutikimo užklausą sandorio pradžioje tampa vis mažiau prasmingas.[174] Nors DI technologijos kelia daugelį šių iššūkių, pasvarstytina, jog jos taip pat gali būti ir išeitis, pateikiant naujus būdus, kaip paaiškinti, kas vyksta kiekviename apdorojimo sluoksnyje, ar sukurti specifines pritaikytas platformas racionaliam sutikimui duoti.

Iš kitos perspektyvos, kaip išskiria Matthew Humerick[175], atkreiptinas dėmesys ir į BDAR įtvirtintą sutikimo atšaukimą. Duomenų subjektai pasilieka teisę bet kuriuo metu atšaukti sutikimą[176], o tam tikrais atvejais gali pasinaudoti teise apriboti savo duomenų tvarkymą.[177] Tokios teisės yra nepalankios DI raidai, nes *post factum* ribojamas duomenų,

[172] NORBERG, P. A. *et al*. The privacy paradox: Personal information disclosure intentions versus behaviors, *Journal of Consumer Affairs*, Vol. 41, No.1, 2007, p. 100–126 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x>.
[173] PEACOCK, S. E. How web tracking changes user agency in the age of Big Data: The used user, *Big data and society*, Vol. 1, No. 2, 2014, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://journals.sagepub.com/doi/10.1177/2053951714564228>.
[174] *Big data, artificial intelligence, machine learning and data protection*, Information Commissioner's Office, 2017, p. 30 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.
[175] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 405-407 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[176] BDAR 7 str.
[177] *Ibid*. 18 str.

iš kurių DI gali mokytis, kiekis. Organizacija gali surinkti didelį kiekį duomenų vien tik mašininio mokymosi tikslais. Jei kiekvienas duomenų subjektas sutiktų, šis DI modelis būtų teisėtas ir nevaržomas, nepaisant jo metodikos. Tačiau tokiu atveju, jeigu duomenų subjektas arba jų grupė atšauktų tokį sutikimą – nors išankstinis duomenų tvarkymas būtų teisėtas[178], tolesnis šių konkrečių duomenų punktų tvarkymas ir mokymasis iš jų – būtų BDAR pažeidimas. Kadangi DI mokymosi procese ir toliau naudoja ankstesnius duomenis, kaip įgytą patirtį vystant intelektą, kyla klausimas, kaip vienu metu sustabdyti DI mokymąsi iš šių duomenų, nedarant poveikio ankstesnei jo raidai ir raidos kokybei, nes bet koks tolesnis mokymosi apdorojimas būtų pradinio rinkinio visumos, kuriame yra atsiimti duomenys, darinys. Vietoj to, DI turi gauti naujų duomenų, kad vėl išmoktų savo funkciją, nebent duomenų apdorojimo blokas galėtų kaip nors izoliuoti mokymosi linkmę, į kurią įtraukti šie pašalintini duomenys.

Galima daryti išvadą, kad sutikimas, kaip vienas iš pagrindinių teisėtumą užtikrinančių duomenų tvarkymo pagrindų, turi daug probleminių aspektų sutikimą duodant duomenų tvarkymui DI pagrindu. Dėl per didelės atskirties tarp sudėtingų duomenų tvarkymo procesų ir duomenų subjekto gebėjimo juos įvertinti, teisėtumui užtikrinti reikalaujamas skaidrumas yra iš esmės neracionalus bei veda prie iš esmės duodamo nesąmoningo sutikimo praktikos, net ir leidžiant subjektui susižinoti prieš sutinkant. Antra problematika slypi sutikimo atsiėmimo poveikyje DI procesams – aktualus reguliavimas kelia nuolatinę atsakomybės riziką tiems, kurie ir toliau mokosi iš neteisėtai apdorotos informacijos.[179]

3.1.1.2 Sąžiningumas

Nei duomenų apsaugos teisėje, nei kitose teisės srityse sąžiningumo principo turinys nėra išsamiai ir oficialiai apibrėžtas, tačiau bendra prasme sąžiningumo principas reiškia duomenų valdytojo ir tvarkytojo pareigą sąžiningai tvarkyti duomenis. Vadovaujantis šiuo principu siekiant duomenų tvarkymo tikslų, J. Zaleskis išskiria[180], jog duomenų valdytojas privalo (i) atsižvelgti į duomenų subjekto interesus ir pagrįstus lūkesčius,[181] (ii) duomenis tvarkyti darniai ir proporcingai ir (iii) nepiktnaudžiauti duomenų tvarkymu.[182] Kuomet DI

[178] BDAR 7 str. 3 d.
[179] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 405-407 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[180] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 115.
[181] BDAR 1 str. 2 d.
[182] PETRAITYTĖ, I. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013, P. 97.

kontekste, šis principas patikimo DI etikos gairėse[183] aiškinimas kiek detaliau, išskiriant du lygmenis:

1. Materialiniu lygmeniu tai yra (i) įsipareigojimas užtikrinti vienodą ir sąžiningą naudos ir sąnaudų paskirstymą (atsispindi sanglauda su proporcingumo principu) ir (ii) užtikrinti, kad asmenys ir grupės nebūtų nepagrįstai šališkai vertinami, diskriminuojami ir stigmatizuojami (šališkumo aspektas); (iii) naudotojai niekada neturėtų būti apgaudinėjami ir neturėtų būti mažinama jų pasirinkimo laisvė (autorės nuomone, tai ryškiausias sąžiningumo aspektas, nors ir kvestionuotino ir daugiau teorinio įgyvendinimo); (iv) DI specialistai turėtų laikytis priemonių ir tikslo proporcingumo principo (jau konkreti nuorodą į proporcingumą), bei (v) atidžiai analizuoti, kaip suderinti besikertančius interesus ir tikslus (interesų derinimo poreikis atspindi tam tikrą tarpusavio atsakomybę, socialinį atsakingumą).
2. Procedūriniu lygmeniu turi būti užtikrinama (i) galimybė ginčyti DI sistemų ir jas valdančių žmonių sprendimus ir naudotis teisių gynimo priemonėmis; (ii) už sprendimą atsakingą asmenį turi būti galima identifikuoti ir (iii) sprendimų priėmimo procesas turėtų būti paaiškinamas. Vadinasi DI programų ir paslaugų atžvilgiu, duomenų apdorojimo sistemų ypatybės turi sudaryti sąlygas duomenų subjektams iš tikrųjų suprasti, kas vyksta su jų duomenimis, net gi neatsižvelgiant į teisinį duomenų tvarkymo pagrindą. Kaip programos yra suprojektuotos veikti ir kaip asmens duomenys yra naudojami yra svarbus faktorius sprendžiant dėl sąžiningumo.[184] Taigi procedūriniu aspektu iš esmės referuojama į teisinės gynybos užtikrinimą bei DI veiklos kontekste paties proceso paaiškinamumą.

Tiek pagal pačius jau BDAR nustatytus, tiek minėtose gairėse apibrėžtus materialinius ir procedūrinius aspektus yra akivaizdus sąžiningumo principo neatsiejamumas nuo kitų duomenų teisės principų. Turint omenyje tokį principų reguliavimo aptakumą ir persipynimą, sutiktina, jog dėl duomenų tvarkymo atitikmens

[183] 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Policy and investment recommendations for trustworthy Artificial Intelligence, 13 p. 52 punktas [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>. Nors lietuviškame vertime naudojama *teisingumo,* o ne *sąžiningumo* sąvoka, šios terminijos dažnam painiojimui teisiniuose vertimuose iš anlgų kalbos duomenų apsaugos kontekste, šiame darbe laikytina, kad pagal bendrą praktiką angl. *fairness* – sąžiningumo principo atitikmuo.

[184] *Big data, artificial intelligence, machine learning and data protection,* Information Commissioner's Office, 2017, p. 38 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

sąžiningumo principui, kiekvienu atveju iš esmės vertintina tik pagal konkrečias susiklosčiusias aplinkybes.[185]

Didesnės analizės verta šališkumo ir diskriminacijos grėsmė užtikrinant sąžiningumą. Organizacijos, diegiančios DI programas, turi žinoti apie šio diegimo poveikį ir reikšmę ne tik konkretiems duomenų subjektams ir jų teisėms bei laisvėms, bet taip pat bendruomenėms ir visuomenės grupėms.[186] Kai kur net gi išskiriama, jog sąžiningumas, tarp kitų esminių etinių DI iššūkių iš esmės ir formuluoja pareigą, jog kuriant DI, reikėtų susilaikyti nuo duomenų rinkinių, kuriuose yra diskriminacinių šališkumų, naudojimo.[187] Visgi, bendrai samprotaujama ir tai, jog visi algoritmai tam tikra prasme yra šališki, nes jie visada yra visuomenės pasirinkimų ir vertybių visumos atspindys – per konfigūracijas, veikimo kriterijus arba mokymo įvesties duomenis“.[188]

Europos Tarybos ataskaitoje dėl DI[189], išskiriama, jog šališkumas gali būti susijęs (i) su metodais (pvz., DI nustatymų, metodų šališkumu), (ii) tyrimo objektu (pvz., socialiniu šališkumu, paremtu ankstesnėmis šališkumo tendencijomis arba nepakankamu kai kurių kategorijų atstovavimu), (iii) duomenų šaltiniais (pvz., jų šališku parinkimu) arba (iv) už analizę atsakingu asmeniu (pvz., šališkumu tvirtinant DI sprendimus). To išeiga DI tvarkant duomenis pagal susikurtą patirtį – galima diskriminacija tam tikrų asmenų grupių atžvilgiu.

Taigi, jau kuriant ir diegiant mašininio mokymosi procesus mašinų mokymosi procesai gali būti sukurti „šališki“. Kiekvienas programuotojas gali sąmoningai arba nesąmoningai programuoti savo šališkumą didelę galią turinčioms sistemoms, kurios pagal priskirtas funkcijas gali nulemti nuo to, kas gauna darbą ar paskolą, iki to, kam suteikiamas

---

[185] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 114.

[186] Pažymėtina, kad kai kurie autoriai iškėlė kolektyvinio privatumo klausimą, ypač dėl profiliavimo poveikio visuomenės grupėms. Žr. pvz. MANTELERO, A. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, *Computer Law & Security Review* Volume 32, Issue 2, April 2016, p. 238-255 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/295894703_Personal_data_for_decisional_purposes_in_the_age_of_analytics_From_an_individual_to_a_collective_dimension_of_data_protection>.

[187] MISHRA, S. *et al*. Artificial Intelligence Index 2019 annual report, Stanford Human Centered Artificial Intelligence, p. 271 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf>.

[188] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, p. 43 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

[189] 2018 m. spalio 15 d. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) Report on Artificial Intelligence, *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, T-PD(2018)09Rev [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808e6012>.

lygtinis paleidimas. Vienas iš siūlomų sprendimų tokiu atveju yra didesnė kodavimo įvairovė. „Google“ vadovai pripažino[190], kad DI sritis „neturi reikiamos įvairovės“, „tik kurdamos įtraukią kultūrą įmonės gali judėti teisingesnių sistemų kūrimo link[191]. Taigi siekiant įvairiapusių interesų užtikrinimo ir socialiai atsakingų sprendimų, gali būti svarbus ne tik užduočių ir kitų procesinių duomenų tvarkymo reikalavimų kokybiškas formulavimas ir vykdymas, tačiau ir pakankamos įvairovės tarp įgyvendinančiųjų asmenų užtikrinimas. Praktiškai tai gali atrodyti taip, jog bendrovės samdančios programuotojus siekiant išvengti vienpusių interesų atstovavimo, turi vykdyti pozityvią diskriminaciją užtikrinant tam tikras darbuotojų kvotas pagal kategorijas.

Be kita ko, tiesiogiai ar netiesiogiai įdiegiant šališkumą algoritmui, parengti naudojamų duomenų kiekis ir kokybė, įskaitant jų šaltinių patikimumą ir ženklinimą, taip pat gali turėti didelės įtakos profilių kūrimui, veido atpažinimui ar emocijų nustatymui. Praktikoje toks diskriminacinis sąžiningumo principo pažeidimas atsispindėjo per tokius atvejus, kaip antai, kuomet: DI apdirbant biometrinius duomenis „Google“ veidų atpažinimo algoritmas juodaodžius identifikavo kaip gorilas[192]; Kinijoje moteris teigė, kad jos bendradarbis sugebėjo atrakinti jos „iPhone X“ naudodamas savo „Face ID“[193] ir kita.

Galiausiai pažymėtinas šališkumo formavimosi pagrindas – pačių vartotojų elgsenos virtualioje erdvėje aspektas. Tai – iš esmės yra DI mokymosi medžiaga. Iliustracijai – 2014 m. „Google“ vartotojas į paiešką įvedė „English major who taught herself calculus“, „Google“ pasiūlė pataisyti užklausą į „English major who taught himself english“. Tokio atvejo priežastis, anot „Google“, buvo tai, jog „taught himself calculus“ (liet. *save patį mokė skaičiuoti*) vartotojų buvo ieškota 70 kartų daugiau, nei kad „taught herself calculus“ (liet. *save pačią mokė skaičiuoti*), todėl algoritmai manė, jog „*himself*“ variantas buvo teisingas.[194] Tad net gi pasyviai atliekami veiksmai algoritmams identifikuoja visuomenės valingus ar nevalingus polinkius rinktis vienus variantus dažniau

[190] LEE, D. *Google executive warns of face ID bias*, BBC, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.bbc.com/news/technology-44977366>.
[191] POLONSKI, V. *Mitigating algorithmic bias in predictive justice: 4 design principles for AI fairness*, Towards Data Science, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/EtIi5R8>.
[192] GUYNN, J. *Google Photos labeled black people 'gorillas'*, USA today, 2015 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eu.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465/>.
[193] NEAL, B. *A Woman In China Claims That Her iPhone X Was Unlocked By A Coworker's Face, & It's Raising Questions About Diversity In Tech*, Bustle, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/StIiMnE>.
[194] MCMANUS, E. *Why did this simple Google Search get retweeted 3,500 times?* Ideas Ted, 2014 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ideas.ted.com/why-did-this-simple-google-search-get-retweeted-3500-times/>.

nei kitus, kas gali sąlygoti tam tikrą diskriminacinę išdavą, nors ir be jokio pirminio diskriminacinio užmojo. Nesant DI sistemose specifiškai suprogramuotų saugiklių, DI neturintis aukšto lygio bendro suvokimo (angl. *common sense*), to negali numatyti ir išvengti.

3.1.1.3 Skaidrumas

Nors skaidrumo definicija BDAR pažodžiui neįtvirtinta, 39 konst. d. p. pateikiama informacija apie skaidrumo, kaip vieno iš pagrindinių principų, reikšmę ir poveikį duomenų tvarkymo srityje. Trys esminės sritys, kurioms principas taikomas: (i) informacijos teikimui duomenų subjektams, susijusiems su sąžiningu tvarkymu; (ii) duomenų valdytojų bendravimui su duomenų subjektais, atsižvelgiant į jų teises pagal BDAR; (iii) vertinimui kaip duomenų valdytojai palengvina duomenų subjektų naudojimąsi jų teisėmis.[195] BDAR skaidrumo reikalavimai taikomi neatsižvelgiant į teisinį duomenų tvarkymo pagrindą ir taikomi visą apdorojimo gyvavimo ciklą,[196] tad galima teigti, jog skaidrumo principas visapusiškai veikia asmens duomenų tvarkymą ir įgalioja duomenų subjektus laikyti duomenų valdytojus ir duomenų tvarkytojus atskaitingais bei įgyvendinti galimybę kontroliuoti savo asmens duomenis. Pvz., tai ypač aktualu, kaip anksčiau minėta, duodant ar atšaukiant informacija pagrįstą sutikimą tvarkyti duomenis arba imantis veiksmų įgyvendinti savo duomenų subjekto teises. Skaidrumo principo pagrindu duomenų subjektams turi būti aišku, kaip su jais susiję asmens duomenys yra renkami ir naudojami, kaip su jais susipažįstama arba kaip kitaip jie yra tvarkomi, taip pat kokios apimties tie asmens duomenys yra ar bus tvarkomi.[197]

Skaidrumo reikalavimas – kaip teisėtumo, sąžiningumo ir skaidrumo principo sudedamoji dalis – yra užtikrinamas ir per BDAR nustatytas duomenų subjektų teises, kaip antai 12 str. numatytą teisę į skaidrų informavimą ir pranešimą bei 15 str. įtvirtintą duomenų subjekto teisę susipažinti su duomenimis. Informacija turi būti lengvai prieinama ir suformuluota aiškia ir suprantama kalba, kad asmenys galėtų naudotis savo teisėmis, įtvirtintomis BDAR. Automatizuoto sprendimų priėmimo kontekste duomenų subjekto požiūriu – bet kokia prasminga informacija apie automatizuoto sprendimų priėmimo logiką, įskaitant profiliavimą, ir numatomi tokio apdorojimo padariniai, skaidrumo

[195] 2018 m. balandžio 11 d. Article 29 WP Transparency Guidelines, wp260rev.01, p. 4 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>.
[196] BDAR 12 str.
[197] *Ibid*. 13-14 str., 60-62 konst. d. p.

aspektu, gali priklausyti nuo teisės susipažinti su atitinkamais asmens duomenimis, įskaitant metaduomenis.[198]

ES, DI šaltinių kontekste, patikimo DI etikos gairėse išdėstoma, jog skaidrumo reikalavimas yra glaudžiai susijęs su paaiškinamumo principu ir apima DI sistemai svarbių elementų – duomenų, sistemos ir verslo modelių, skaidrumą. Pats principas aiškinimas per tris sudedamąsias – atsekamumą, paaiškinamumą ir informacijos sklaidą. EK komunikate dėl pasitikėjimo į žmogų orientuotu DI didinimo, vertinant skaidrumo svarbą, pozicija išlaikoma ir atspindimi tapatūs principo aspektai.[199]

DI atveju, duomenų valdytojas ypač reikalingas[200], kad informuotų apie duomenis dėl automatizuoto sprendimų priėmimo buvimo ir pateiktų reikšmingą informaciją apie susijusią logiką, tokio duomenų tvarkymo svarbą ir numatomas pasekmes. Tai, kas suprantama kaip „prasminga informacija“ apie „logiką“, turi būti vertinama duomenų subjekto požiūriu. Pagrindiniai skaidrumo komponentai yra informacijos prieinamumas ir suprantamumas. Norvegijos DPA pabrėžia skaidrumo reikalavimo vykdymo sudėtingumą kuriant ir naudojant DI, nes sunku suprasti ir paaiškinti, kaip konkrečiame procese informacija tarpusavyje siejama ir vertinama.[201] Prancūzijos duomenų apsaugos valdyba atkreipia dėmesį į specialistų rekomendaciją teikti pirmenybę, kaip įvardija, algoritmo paaiškinimui ar suprantamumui, o ne skaidrumui: „Visiems turėtų būti sudaryta galimybė suprasti šią logiką, kuri turi būti paaiškinama žodžiais, o ne kodais“.[202] Taigi daug prasmingesnis yra aukšto lygio, netechninis sprendimų priėmimo proceso aprašymas pagal tuo siekiamą tikslą, o ne *per se* proceso skaidrumas kaip procedūrinis reikalavimas, pagal šią poziciją. Remiantis Vokietijos pozicija, sprendžiama, jog pakanka labai paprastai informuoti apie numatomus padarinius, t. y., pakaktų paaiškinti, kaip žemas kreditingumo reitingas gali paveikti mokėjimo galimybių pasirinkimą. Ankstesnės Vokietijos jurisprudencijos ir Vokietijos komentaruose dėl BDAR pripažįstamas paaiškinimo tipas

---

[198] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

[199] 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Policy and investment recommendations for trustworthy Artificial Intelligence [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>.

[200] BDAR 13 str. 2 d. f p. ir 14 str. 2 d. g p.

[201] *Artifical intelligence and privacy*, Norvegian Data Protection Authority, Datatilsynet, 2018, p. 19. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

[202] *Comment permettre à l'homme de garder la main?*, Commission nationale informatique et libertes, 2017, p. 51 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf>.

ribojamas pagrindinių duomenų valdytojo interesų, pvz., komercinių paslapčių apsaugos arba vartotojų „lošimo sistemos“ prevencijos. Procesas, kurį naudoja algoritmai, neturi būti atskleistas. Tokie komentarai dėl BDAR grindžiami bendru Duomenų apsaugos direktyvos aiškinimu ir ankstesne jurisprudencija dėl teisės susipažinti. Šiuo atveju, pasak komentatorių, duomenų valdytojams nereikia išsamiai paaiškinti konkretaus sprendimo suteikti duomenų subjektams „reikšmingą informaciją apie susijusią logiką“ (BDAR 15(1)h str.) motyvų ir aplinkybių.[203] Taigi valstybių praktika aiškinant skaidrumą yra kiek skirtinga.

Literatūroje pasigirsta ir iš esmės neigiamo vertinimo kvestionuojant ar skaidrumo principas yra reikalavimas *ex post* paaiškinti automatizuotus sprendimus – „ilgalaikė žmogaus teisių ir laisvių sveikata tiesiogiai ar net didžiąja dalimi nepriklausys nuo tokios teisės prieinamumo – skaidrumas nėra sidabrinė kulka, kuri būtinai išlaikys algoritminį reguliavimą sąžiningą“.[204] Kyla tam tikras pavojus, kad mokslinių tyrimų ir teisėkūros pastangos bus skirtos tam, kad būtų užtikrintos teisės į skaidrumą, nors tai praktiškai gali būti neįmanoma ir neatitikti vartotojų poreikių. Kaip rodo finansų ir kreditų sektorių istorija, teisės į skaidrumą nebūtinai užtikrina esminį teisingumą ar veiksmingas teisių gynimo priemones. Kalbama apie pavojų sukurti „beprasmio skaidrumo“ paradigmą, kuri atitiktų jau gerai žinomą „beprasmio sutikimo“ įvaizdį.[205]

Vadinasi, DI kontekste siekiant sukurti būtinas BDAR diktuojamas skaidrumo sąlygas yra būtini tiek teisiniai ir procedūriniai sprendimai, tiek techniniai suderinimai su DI technologija, nes kitu atveju kyla rizika pažeisti kitus visuomenės gėrius ir asmenų teises. Modelių ir procesų neskaidrumas ypač rizikingas turint omeny intelektinės nuosavybės, komercinių ar net valstybės paslapčių ir kitos jautrios informacijos apsaugą. Skaidrumas DI tvarkant asmens duomenis didelį vaidmenį atlieka kaip DI atskaitomybės jį patį pasitelkiančiam duomenų valdytojui ir atskaitomybės pačiam duomenų subjektui – skaidrumas veikia kaip duomenų tvarkymo kontrolės elementas. Jis leidžia atsekti ir tinkamai paskirstyti atsakomybę už sprendimų priėmimo nesėkmes ar šališkas prognozes.

***

Šie trys principai arba pagal formuluotę kaip vienas teisėtumo, sąžiningumo ir skaidrumo jungtinis principas yra fundamentalus pagrindas visam DI kūrimui ir veikimui,

[203] WACHTER, S. et al. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469>.
[204] YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019.
[205] YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 259.

kiek atliekama duomenų tvarkymo funkcija. Pagrindinis šio jungtinio principo tikslas pagal atskirus elementus gali būti išskirstomas ir suponuoja skirtingą taikymo DI problematiką, visgi, akivaizdu, jog kiekvieno dedamojo principo turinio išpildymas duomenų apsaugos reguliavimo kontekste yra neatsietinas ir nuo kitų įgyvendinimo.

3.1.2 Duomenų tvarkymo tikslo apribojimo principas

Duomenų tvarkymo tikslo apribojimo principo pagrindu asmens duomenys turi būti renkami (i) nustatytais, (ii) aiškiai apibrėžtais bei (iii) teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderintu būdu.[206] Šio principo tikslas – apsaugoti duomenų subjektą duomenų valdytojams nustatant ribas, kurių neperžengdami jie gali naudoti duomenų subjektų duomenis ir užtikrinti tvarkymo sąžiningumą.[207] Tikslo apribojimo principas yra glaudžiai susijęs su skaidrumu, nuspėjamumu ir sąžiningumu.

Praktikoje DI apdirbant asmens duomenis vadovaujantis šiuo principu pagal paprastą pavyzdį yra draudžiama analizuoti ir išgauti biometrinius duomenis iš „Siri“ ar „Alexa“ įrašytų fizinių asmenų balsų.[208] Problematika taikant principą DI atsispindi tame, jog mašininio mokymosi sistemos pagal savo priedermę – sukurtos apdirbti kuo daugiau duomenų ir iš jų išvesti kuo daugiau naujų taisyklių ar prognozių. Todėl tikslų apribojimo principas išsiskiria savo ribojančiu poveikiu DI – jo laisvei daryti atradimus ir naujoves, jei tai nėra tiesiogiai suderinama su pirminiu duomenų tvarkymo tikslu.

Visgi Ronald Leenes ir Silvia De Conca linkę išskirti, jog viena vertus, duomenų tvarkymo tikslo apribojimo principas aiškiai riboja asmens duomenų tvarkymą, nes pagal jį reikalaujama iš anksto nurodyti tvarkymo tikslus, šie tikslai be to turi būti teisėti, tačiau, antra vertus, duomenų valdytojams tuo kaip tik suteikiama daug laisvės – jiems leidžiama tvarkyti asmens duomenis (jei laikomasi kitų reikalavimų) jų pačių nurodytais tikslais. Kitaip tariant, kol duomenų valdytojas yra skaidrus ir atviras duomenų tvarkymo tikslams, jis turi daug laisvės. Iliustraciniam pavyzdžiui mokslininkai pateikia intelektualiojo namų asistento atvejį – vienas iš balso duomenų rinkimo tikslų gali būti „pagerinti prietaiso

[206] BDAR 5 str. 1 d. b p., 39 konst. d. p.
[207] 2013 m. balandžio 3 d. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.
[208] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, p. 47 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

savininkų kalbos atpažinimą“.[209] Taigi visą principo taikymo problematiką galima apspręsti tiklsingai numatant duomenų valdytojo interesus aprėpiančius duomenų naudojimo tikslus, kas teisiškai gali būti kritiškai vertinama ryšium su kitais duomenų apsaugos principais, tačiau *per se* praktiškai atlikti itin paprasta, turint omenyje dažną vartotojų nesąmoningą sutikimą su duomenų tvarkymo užklausimais.

Be kita ko, atkreiptinas dėmesys, jog sprendžiant, ar tolimesnis asmens duomenų tvarkymas yra suderinamas pagal BDAR reguliavimą, pateikiama, jog, tikslų ribojimo principas netrukdo pakartotinai naudoti asmens duomenų mokslo ir (arba) statistikos tikslais.[210] Asmens duomenų naudojimui moksliniams tyrimams taikomos specialios BDAR 89 str. ir atitinkamos apsaugos priemonės, įskaitant duomenų subjekto teisių užtikrinimą ir techninių bei organizacinių saugumo priemonių taikymą. Todėl, autorės nuomone, duomenų tvarkymo tikslo apribojimo principas savaime nėra ribojantis inovacijų ir BDAR reguliavimu sudaromos sąlygos išvengti pernelyg griežto ribojimo vertinant iš tinkamos teisinės aplinkos mokslinei pažangai užtikrinimo perspektyvos. Visgi, kalbant apie mokslinius tyrimus, susijusius su DI, sutiktina su Lilian Mitrou[211], jog čia reikia turėti omenyje ir atskirą problematiką, jog praktiškai gali būti sunku atskirti (mokslinę) plėtrą ir įprastą DI taikymą, nes DI modeliai nuolat vystosi ir tobulėja maitindamiesi vis daugiau (asmeninių) duomenų, taigi sunku atriboti „kur baigiasi moksliniai tyrimai ir prasideda naudojimas“.[212]

3.1.3 Duomenų kiekio mažinimo principas

Duomenų kiekio mažinimo principo pagrindu asmens duomenys turi būti (i) adekvatūs, (ii) tinkami ir (iii) tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi. Tvarkomų duomenų kiekį turi apibrėžti iš anksto duomenų valdytojo įvardytas duomenų tvarkymo tikslas ir asmens duomenys turėtų būti tvarkomi tik jeigu asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis.[213] Todėl duomenų valdytojai privalo

[209] NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018. P. 289.
[210] BDAR 50 konst. d. p.
[211] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, p. 48 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.
[212] *Artifical intelligence and privacy*, Norvegian Data Protection Authority, Datatilsynet, 2018, p. 18. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.
[213] BDAR 39 konst. d. p.

apsvarstyti, ko jiems reikia, kad galėtų pasiūlyti savo paslaugas arba atlikti savo užduotis, ir apdoroti ir saugoti tik minimalų duomenų kiekį, kurio pakaktų šiems tikslams pasiekti. Doktrinoje formuojama pozicija, jog taikant duomenų kiekio mažinimo principą įpareigojama apriboti ne tvarkomų duomenų kiekį iki absoliutaus minimumo, tačiau duomenų rinkimą iki tinkamo lygio, atsižvelgiant į duomenų tvarkymo tikslus.[214] Šis principas taip pat susijęs su duomenų saugojimo trukme – neturi būti saugoma ilgiau nei būtina.

Pagal paties įstatymų leidėjo ketinimus, kaip rašo Tal Z Zarsky, (i) sprendžiama, jog duomenų valdytojui turint prieigą prie mažiau duomenų, jis rečiau pažeidžia duomenų subjekto privatumą, (ii) duomenų valdytojui ilgesnį laiką laikant didelį duomenų kiekį tokie duomenys gali būti kibernetinių grėsmių ir duomenų nutekėjimo objektu, todėl duomenų sumažinimas sumažina šią riziką; (iii) siekiama padidinti duomenų subjekto savarankiškumą savo pačių duomenų atžvilgiu ir (iv) sulaikyti duomenų valdytoją nuo pernelyg didelio ir / ar nepriimtino duomenų naudojimo.[215]

Didelio duomenų kiekio saugojimą galima nesunkiai laikyti privatumo pažeidimu, o argumento, kad duomenys nenaudojami, nepakanka jų išsaugojimui pagrįsti,[216] todėl kyla pareiga užtikrinti tinkamą duomenų tvarkymo tikslų ir duomenų apimties santykį. Taikymo prasme tai ypač aktualu duomenų kaupimui, įprastam valdžios institucijoms ir privačioms pasaulinio masto bendrovėms, surenkančioms daugiau asmens duomenų nei reikalaujama. Pvz., naudojant tokias DI pagrindu veikiančias darbe jau minėtas programas – „Siri“ ar „Alexa“ – surinkti balso duomenys, siekiant pagerinti balso atpažinimą, turėtų būti panaikinti, kai pasiekiamas pakankamas atpažinimo lygis.[217] Tačiau tokie reikalavimai vis dar nėra atsakingai įgyvendinami – remiantis statistikos duomenimis – Jungtinės Karalystės, Prancūzijos ir Vokietijos įmonių tyrime 72 % organizacijų teigė rinkę duomenis, kuriais vėliau nesinaudojo.[218]

---

[214] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 121.

[215] ZARSKY, T. Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646>.

[216] NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018, p. 290.

[217] NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018. P. 290

[218] *Big data, artificial intelligence, machine learning and data protection*, Information Commissioner's Office, 2017, p. 85 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

Turint omenyje technines duomenų tvarkymo galimybes, duomenų kiekio mažinimo principas DI ir didžiųjų duomenų kontekste, vertintina, jog gali būti sunkiai įgyvendinamas ar net gali iš esmės prieštarauti didžiųjų duomenų analizei ir mašininio mokymosi sistemoms, kurios yra pagrįstos, o gal net priklausomos nuo masinio duomenų rinkimo ir galimybės juos pakartotinai sujungti ir pakartotinai naudoti. Su tokia pozicija pasaulio mokslininkų plačiai sutinkama. Didžiųjų duomenų pagrindas prieštarauja šiam principui, nes didieji duomenys pagal koncepciją suteikia galimybę saugoti duomenis nenumatytam būsimam naudojimui, kuris tiesiogiai prieštarauja duomenų minimizavimo principui, pagal kurį duomenys turi būti saugomi ne ilgiau, nei būtina pradiniam jų rinkimo tikslui.[219] Dabartinė duomenų mažinimo ir didelių duomenų padėtis yra taisyklių, prieštaraujančių rinkai, padėtis – teigia Oluwayomi A. Ajibade.[220] Tai laikoma priešprieša didiesiems duomenims,[221] kurie leidžia rinkti ir saugoti didelį duomenų kiekį, o duomenų mažinimas leidžia rinkti ir saugoti mažiau duomenų nei reikia, todėl šios dvi sąvokos tampa nesuderinamomis.[222] Pažymėtina, jog šį nesuderinamumą dar labiau sustiprina duomenų subjekto teisė prašyti ištrinti jo duomenis[223]. Sutiktina su vertinimu[224], jog tai išties apsunkina didelių duomenų naudotojų lūkesčius, kai duomenų negalima rinkti ir laikyti tolesniam naudojimui.

Principas sunkiai koreliuoja su DI technologija ir tuo aspektu, jog duomenų valdytojams kyla uždavinys nuo pat pradžių apibrėžti (i) tvarkymo tikslus, į kuriuos nėra lengva atsakyti, nes paprastai neįmanoma numatyti, ko algoritmas išmoks, ir (ii) numatyti

---

[219] International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics, 2014, p. 16 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2014/08/working_paper_onbigdataandprivacyaufenglisch.pdf.download.pdf/working_paper_onbigdataandprivacy.pdf>.

[220] AJIBADE, O. *A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape*, 2018, p. 28. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330397864_A_Critical_Appraisal_of_Big_Data_Analytics_within_the_General_Data_Protection_Regulation_GDPR_Landscape>.

[221] International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics, 2014, p. 6 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2014/08/working_paper_onbigdataandprivacyaufenglisch.pdf.download.pdf/working_paper_onbigdataandprivacy.pdf>.

[222] 2014 m. rugsėjo 16 d. Article 29 Data Protection Working Party Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.pdpjournals.com/docs/88352.pdf>.

[223] BDAR 17 str.

[224] AJIBADE, O. *A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape*, 2018, p. 37 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330397864_A_Critical_Appraisal_of_Big_Data_Analytics_within_the_General_Data_Protection_Regulation_GDPR_Landscape>.

duomenis, kurie bus svarbūs, taip apribojant į mokymą ar modelio naudojimą įtrauktinų ir vėliau paliktinų duomenų kiekį.[225] Šiuo požiūriu duomenų mažinimo principas yra susijęs tiek su duomenų nusimatytinu kiekiu, tiek su apdorojimo veikla. Laikantis duomenų minimizavimo principo, ribojamas įsikišimo į asmens (informacinį) privatumą mastas arba net sąlygojimas susilaikymo nuo pačių DI metodų naudojimo, jei duomenų tvarkymo tikslas gali būti pasiektas mažiau invaziniu būdu į asmens privatumą.[226]

Taigi šis principas prieštarauja ir iš esmės yra itin priešiško poveikio DI veikimo procesams. Kai apdirbami duomenys yra naudingi, principo taikymas sumažina jų galimą naudojimą ateityje. Antra vertus, duomenų mažinimo principo laikymasis yra gero duomenų valdymo proceso dalis, padedanti gerinti duomenų kokybę ir duomenis atrinkti. Su dideliais duomenimis ateina didelės žinios, kurios lemia ne tik DI sistemos, tačiau ir visuomenės vystymąsi reaguojant į DI pateikiamas išvadas ir priimamus sprendimus. Visgi, duomenų sumažinimas gali kiek trukdyti šiam optimistiškam požiūriui.[227]

3.1.4 Pritaikytosios ir standartizuotosios duomenų apsaugos principas

Vienas ryškiausių pastarojo meto su BDAR įsigaliojimu kilusios duomenų apsaugos reformos bruožų yra konkrečių ir platesnių reikalavimų, susijusių su pritaikytąja ir standartizuotąja duomenų apsauga, nustatymas. Pagal BDAR reguliavimą duomenų valdytojas turi (i) taikyti tinkamas technines ir organizacines priemones, kuriomis siekiama veiksmingai įgyvendinti duomenų apsaugos principus ir į duomenų tvarkymą įtraukti būtinąsias apsaugos priemones, jog jis atitiktų duomenų apsaugos teisės nuostatas, (ii) užtikrinti, kad standartizuotai būtų tvarkomi tik tie asmens duomenys, kurie yra būtini siekiant kiekvieno konkretaus duomenų tvarkymo tikslo[228]. Šios pareigos akivaizdžiai apima ir kitų duomenų apsaugos principų, t. y. minimizavimo ir proporcingumo, bei

[225] *Artifical intelligence and privacy*, Norvegian Data Protection Authority, Datatilsynet, 2018, p. 18. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.
[226] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, p. 49-50 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.
[227] AJIBADE, O. *A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape*, 2018, p. 37 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330397864_A_Critical_Appraisal_of_Big_Data_Analytics_within_the_General_Data_Protection_Regulation_GDPR_Landscape>.
[228] BDAR 25 str. 1-2 d.

numatytų duomenų prieinamumo apribojimų užtikrinimo reikalavimą. Kaip rašo Lee A. Bygrave – reglamentu siekiama ne tik „apsisaugoti nuo mašinos“, bet ir ją kurti.[229]

Tinkamam šio gana neapibrėžtai suformuluoto principo vertinimui svarbu suvokti jo įtvirtinimo kontekstą ir pagrindus. Europos mokslo ir naujųjų technologijų etikos grupė pabrėžė, jog „DI ir robotikos taikymas neturėtų kelti nepriimtinos žalos rizikos žmonėms ir nekelti pavojaus žmogaus laisvei ir autonomijai“.[230] Kaip tik inovatyviosios technologijos (i) turėtų būti skirtos pagrindinių teisių ir vertybių apsaugai, (ii) plėtojamos siekiant „tarnauti žmonijai“,[231] (iii) sudaryti palankesnes sąlygas žmonijos vystymuisi ir (iv) netrukdyti ar nekelti žmonėms pavojaus. Kitaip tariant, DI technologijos turėtų būti kuriamos, plėtojamos ir naudojamos atsižvelgiant į pagrindines žmogaus teises ir laikantis sąžiningumo principo. Nesusiejus DI technologijų su pagrindiniais konstituciniais principais, atsirastų „plačiai paplitusi įstatymų nepaisymo kultūra ir kiltų pavojus demokratijai“.[232] Analogiškai EK priimtoje Baltojoje knygoje[233] atkreipiamas ypatingas dėmesys į tai, jog DI naudojimas gali turėti įtakos vertybėms, kuriomis grindžiama ES, ir lemti pagrindinių teisių pažeidimus. Ši rizika gali kilti dėl bendro DI sistemų projektavimo trūkumų (taip pat ir dėl žmonių priežiūros) arba dėl duomenų naudojimo netaisant galimo šališkumo[234] (šališkumo principo atspindys). Kai projektavimo etape negalima užkirsti kelio rezultatams arba jų numatyti, rizika kyla ne dėl pradinio sistemos dizaino trūkumų, o dėl praktinio koreliacijų ar modelių, kuriuos sistema nustato dideliame duomenų rinkinyje, poveikio.[235] Taigi, iš esmės principas įtvirtinamas sprendžiant, jog duomenų apsauga turėtų būti tinkamiau įtraukta į informacines technologijas ir pagal informacinių technologijų veikimą. BDAR 25 str. laikytinas bandymu įtraukti ES duomenų apsaugos teisės vertybes į informacinių sistemų sandarą. [236]

---

[229] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 248.

[230] European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems*, p. 17 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>.

[231] BDAR 4 konst. d. p.

[232] NEMITZ, P. Constitutional Democracy and Technology in the age of Artificial Intelligence, *Royal Society Philosophical Transactions A*, 2018, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234336>.

[233] 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final, p. 17 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.

[234] *Ibid*. p. 11.

[235] *Ibid*. p. 12.

[236] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 255-258.

Su principo pritaikomumo problematika pirmiausia susiduriama vertinant patį principo adresatą. Galima laikyti, jog straipsnio reikalavimai nustatomi (i) asmens duomenų valdytojams, kurie numato asmens duomenų tvarkymo tikslus, sąlygas ir priemones[237] ir (ii) asmens duomenų tvarkytojams – subjektams, kurie tvarko duomenų valdytojų vardu.[238] Tai, kad straipsnis visų pirma skirtas tik duomenų valdytojams, o dar ir netiesioginiai įsipareigojimai taip pat numatyti duomenų tvarkytojams, kai kurių autorių vertintina kaip pagrindinė straipsnio yda, kuri apskritai pažeidžia duomenų apsaugos teisę.[239] Pozicija grindžiama tuo, jog daugelį esminių sprendimų, kuriais sureguliuojamas informacinių sistemų kūrimas, įskaitant algoritminio reguliavimo struktūrą, išvis priima ne subjektai, atliekantys asmens duomenų valdytojų ar tvarkytojų funkcijas. Nors BDAR ragina duomenų apdorojimo sistemų gamintojus laikytis 25 str. idealų, šis raginimas įtvirtintas preambulėje, kuri savaime nėra teisiškai privaloma.[240]

Aptarus bendrą pritaikytosios ir standartizuotosios duomenų apsaugos principo problematiką, nuosekliam taikymo DI probleminių aspektų atskleidimui principo sudedamosios toliau nagrinėtinos ir skyrium.

3.1.4.1 Pritaikytoji duomenų apsauga

Pagal pritaikytosios duomenų apsaugos reikalavimus orientyras yra būtent tai, jog duomenų apsauga turi būti įtraukta į visą technologijos gyvavimo ciklą: ankstyvąją jos kūrimo stadiją, rengimą galutiniam naudojimui, taikymą ir šalinimą.[241] Asmens duomenims tvarkyti skirtos technologijos ir procesai privalo būti kuriami taip, kad atitiktų duomenų apsaugos principus ir nuostatas.[242] Pritaikytoji duomenų apsauga yra technologijų etikos principo, pagal kurį būtinas vertybėms jautrus projektavimas, išraiškos teisiniame reguliavime forma. Šis principas įtvirtina socialinę ir etinę mokslininkų, išradėjų, inžinierių ir projektuotojų atsakomybę tyrinėjant, išrandant ir projektuojant technologijas, taigi ir DI,

[237] BDAR 4 str. 7 d.
[238] *Ibid*. 4 str. 8 d. Pažymėtina ir tai, jog duomenų valdytojai gali pasitelkti tik tuos duomenų tvarkytojus, kurie pakankamai užtikrina, kad tinkamos techninės ir organizacinės priemonės bus įgyvendintos tokiu būdu, kad duomenų tvarkymas atitiktų reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga pagal BDAR 28 str. 1 d. ir BDAR 81 konst. d.
[239] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 255-258.
[240] *Ibid*.
[241] 2015 m. birželio 16 d. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones – wp231, 01673/15/EN WP 231 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602>.
[242] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019. P. 139.

kurie daro arba galėtų daryti esminį poveikį visuomenei.[243] Reikalavimas dėl pritaikytosios duomenų apsaugos grindžiamas tuo, kad rizikos suvokimas ir atsargumo principas yra labai svarbūs sprendžiant naujųjų technologijų uždavinius.[244]

Nors prie pačių 25 str. tikslų – sunkiai prikibtina – juos įgyvendinant gali kilti sunkumų iš DI reguliavimo pusės. Vieną iš pagrindinių teisinėje literatūroje skirtinų problemų – straipsnio reikalavimų neaiškumas.[245] Iš šios nuostatos kylanti pareiga yra ne tik komplikuota, bet ir labai abstrakti, nesuteikianti aiškumo dėl jos tikslių įgyvendinimo parametrų ir metodikų. Pagal ES 29 str. darbo grupės poziciją, pritaikytosios duomenų apsaugos principas apima tiek duomenų kiekio mažinimą, tiek galimybę kontroliuoti skaidrumą, vartotojui palankias sistemas, duomenų konfidencialumą, duomenų kokybę, duomenų naudojimo ribojimą.[246] Taigi, turiniu iš esmės apimami ir daugybė kitų savaime svarbių ir savo problematiką diktuojančių principų. Be kita ko, taikymo komplikuotumą lemia ir tai, jog principas duomenų apsaugos teisės šaltiniuose pagal turinį įtvirtintas neidentiškai[247], o išorės gairių dėl tokių metodikų, ypač informacinių sistemų kūrėjams, vis dar trūksta.[248]

3.1.4.2 Standartizuotoji duomenų apsauga

Standartizuotosios duomenų apsaugos reikalavimas reiškia, kad technologija turėtų būti sukurta taip, kad būtų išvengta nereikalingo duomenų tvarkymo. Paslaugoms ir produktams turėtų būti parenkami tokie nustatymai, pagal kuriuos būtų vengiama rinkti ir (arba) toliau tvarkyti nereikalingus duomenis,[249] informacinių technologijų sistemos, išmanieji įrenginiai, interneto puslapiai ir kitos duomenų tvarkymo priemonės būtų kuriamos taip, kad jau pradiniai, numatytieji nustatymai padėtų apsaugoti jų vartotojų duomenis.

---

[243] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019. p. 139.

[244] MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018, p. 75-76 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.

[245] Žr. Pvz. BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 255-258.

[246] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 140.

[247] *Ibid*. p. 138.

[248] Pažymėtina, jog EDAV iniciatyva klausimui spręsti priemonių jau imtasi – parengtos pritaikytosios ir standartizuotosios duomenų apsaugos gairės, tačiau, kadangi šiuo metu galutinis variantas po viešosios konsultacijos dar nėra priimtas, darbe apsiribotina galiojančių ir aktualių šaltinių analize, gairių projekto nevertinant [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-42019-article-25-data-protection-design_lt>.

[249] 2015 m. birželio 16 d. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones - wp231, 01673/15/EN WP 231 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602>.

Duomenų tvarkymo priemonių kūrėjai turėtų įvertinti, kurios funkcijos yra būtinos vartotojui, o kurios – konfigūruojamos. Duomenų apsaugai palankūs numatytieji nustatymai turi nesuteikti papildomų produkto atliekamų funkcijų, nebent vartotojas aiškiai jas pasirinktų.[250] Esminius standartizuotosios duomenų apsaugos reikalavimus galima skirti į:

1. Duomenų apimties – pasitelkiamos duomenų tvarkymo priemonės neturi rinkti duomenų apie vartotoją, jeigu jie nėra būtini priemonių funkcionalumui užtikrinti (pastebimas glaudus ryšys su duomenų kiekio mažinimo principu). Pvz., DI atveju išmaniųjų namų robotai, pagal vartotojo rutiną ir įpročius gebantys mokytis ir tobulinti namų aplinką, derinant skirtingų namų prietaisų sąveiką, atitinkamu laiku neturėtų duomenų jutiminiais sensoriais rinkti tose srityse, kurios išeina už vartotojo buitinių interesų ribų, jeigu nėra vartotojo sutikimo.
2. Laiko – suėjus iš anksto apibrėžtam terminui, duomenys duomenų tvarkymo priemonių, turi būti automatiškai ištrinami (vėlgi akivaizdi minimizavimo atmaina).
3. Prieigos – numatytieji nustatymai turėtų būti tokie, kad su duomenimis galėtų susipažinti kiek įmanoma mažiau asmenų, t. y. vartotojų išsamūs duomenys nebūtų matomi viešai ar plačiam asmenų ratui.[251]

Vertintina, jog šio principo reikalavimai yra kiek konkretesni nei pirmiau nagrinėto pritaikytosios duomenų apsaugos, todėl jų taikymas DI gali būti lengviau įgyvendinamas ir prižiūrimas. Visgi, kadangi šiam principui taip pat akivaizdžiai būdinga tai, jog principas yra itin glaudžiai susijęs su kitais duomenų apsaugos teisės BDAR įtvirtintais principais ar net gi nagrinėjant principo turinį juos apima, tai, autorės nuomone, neleidžia užtikrinti aiškumo ir nebrėžia žymių ribų tarp atskirų BDAR kategorijų duomenų valdytojams ir tvarkytojams bei technologijų kūrėjams, kaip vieniems svarbiausių principo tikslų tariamų įgyvendintojų, nors ir įsakmiai, kaip minėta, neįvardintų kaip adresatų. Galiausiai atsižvelgtina į tai, jog, kaip rašo J. Zaleskis, šis principas laikytinas ir atskiru duomenų apsaugos teisės principu, ir sudėtine vieningo pritaikytosios ir standartizuotosios duomenų apsaugos principo dalimi. Taigi atitikimo standartizuotosios duomenų apsaugos

[250] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 142.
[251] Žr. BDAR 25 str. 2 d. bei ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 142.

reikalavimams vertinimas kiekvienu atveju, manytina, jog yra neatsiejamas ir nuo atitikimo pirmosios principo dedamosios – pritaikytosios duomenų apsaugos reikalavimams.

***

Įvertinus šiame skyriuje pateiktus aspektus, pažymėtina, kad BDAR principai iš esmės sudaro reguliavimo pagrindą asmens duomenų tvarkymui ir yra atspirties tašku visų BDAR nuostatų aiškinimui. Šie principai nustato organizacijos, kuri nori dalyvauti asmens duomenų tvarkyme, pareigas, duomenų subjekto atžvilgiu. Toliau nuosekliai pereitina prie reikšmingiausių DI atžvilgiu BDAR įtvirtintų duomenų subjekto teisių poveikio DI vertinimo.

3.2 Duomenų subjekto teisės

BDAR aktualiu reguliavimu sukuriamos ir sustiprinamos teisės, suteikiančios duomenų subjektui savo asmens duomenų „tvarkymo“ kontrolę.[252] Ši kontrolė leidžia jam geriau nuspręsti, kas turi teisę tvarkyti jo duomenis ir kokiais tikslais tai leidžiama. Tvarką, kurios duomenų valdytojai ir duomenų subjektai turi laikytis įgyvendinant duomenų subjektų teises, nustato bendrieji procedūriniai duomenų apsaugos teisės reikalavimai.

Šioje darbo dalyje darbo tikslui pasiekti analizuotinos duomenų subjekto teisės, kurios iš esmės sustiprina būtent DI, apdirbančio asmens duomenis, kontrolę, yra faktorius DI sistemų projektavime ar, kaip kai kurie autoriai linkę vertinti, net gi keliančios grėsmę DI vystymuisi, nes dabartinis jo vystymosi modelis galimai išvis neatitinka BDAR nuostatų.[253] Atitinkamai, toliau vertintina teisės būti pamirštam[254]; teisės į duomenų perkeliamumą[255] ir teisės, kad subjektui nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas reikšmingas sprendimas,[256] turinys ir problematika jas užtikrinant DI kontekste.

[252] BDAR 4 str. 1-2 d.
[253] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[254] BDAR 17 str.
[255] *Ibid*. 20 str.
[256] *Ibid*. 22 str.

3.2.1 Teisė būti pamirštam

Visuomenės nebestebina tai, jog produktai ar paslaugos, kurių ieškoma „Google“, iškart atsiranda kaip skelbimai asmeniniuose socialinės medijos kanaluose. Taip yra todėl, jog asmens elgesys skaitmeninėje erdvėje, kaip ir anksčiau užsiminta šiame darbe, nėra nematomas, juo labiau *per se* sulaik neišnyksta. Atvirkščiai – tai sudaro atskirus duomenis, kuriuos suinteresuoti subjektai, teisėto duomenų rinkimo atveju – turėdami teisėtą pagrindą – renka, saugo ir naudoja. Visgi, pagal esamą BDAR reguliavimą duomenų subjekto naudai yra suteikiama teisė būti pamirštam arba teisė reikalauti ištrinti apie jį surinktus duomenis. Ja pasinaudojus, duomenų valdytojui atitinkamai kyla pareiga tai, nepagrįstai nedelsiant, vykdyti[257]. Kitaip tariant, tokiu atveju, kai duomenų subjektas nebenori dalintis asmenine informacija, jis turi teisę, esant vienam iš BDAR nustatytų pagrindų, paprašyti apie jį surinktus duomenis ištrinti.[258] Visgi, praktine prasme atšaukimas to, kas jau buvo bendrinama internete ar toks duomenų ištrynimas, kad situacijos vertinimas DI apdirbančio asmens duomenis atžvilgiu stotų atgal į *status quo*, technine prasme yra problematiškas ar, kai kuriais atvejais, išvis svarstytina, ar realaus įgyvendinimo. Tai kelia iššūkių patiems didžiųjų duomenų ir mašininio mokymosi veikimo principams.

Reali galimybė sudaryti sąlygas DI įgyvendinti teisę būti pamirštam yra algoritmų, specialiai gebančių *pasimiršti* išmoktas funkcijas be poreikio persikvalifikuoti visą neuroninį tinklą, projektavimas. Tai anksčiau laikyta beveik logiškai nesuderinama su DI veikimo principais, tačiau pastaruoju metu tam įgyvendinti reikalingi technologiniai sprendimai yra vis aktyviau diskutuojami mokslinėje bendruomenėje.[259] Teigiamai vertintina technologijų plėtra ir naujų sprendimų paieška, orientuota į įstatymų leidėjo siekiamus duomenų apsaugos tikslus, tačiau, kita vertus, tai akivaizdžiai rodo, jog kol mokslas dar tik sprendžia tokią pamiršimo galimybę, mašininio mokymosi procesai DI, galimai, yra nuolatinio pažeidimo būsenoje, jei asmenys pasinaudoja savo teise būti pamirštam.

[257] BDAR 17 str. 1 d.
[258] *Ibid*. 17 str. 1 d. a-f p., 8 str. 1 d.
[259] Pvz. 2019 m. paviešintame straipsnyje mokslininkai jau siūlo SISA mokymą – naują sistemą, kuri realiai padeda DI modeliams „pasimiršti“ (angl. *unlearn*) informaciją: „*Neregėtas mastas, kuriuo ML taikomas asmens duomenims, motyvuoja mus ištirti, kaip šią teisę būti pamirštam galima efektyviai įgyvendinti ML sistemoms*“, rašo mokslininkai. BOURTOULE, L. *et al*. Machine Unlearning, University of Toronto∗ , Vector Institute§ , University of Wisconsin-Madison, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://arxiv.org/pdf/1912.03817.pdf>.

Anot Matthew Humerick, teisės būti pamirštam įgyvendinimas net gi labai kenkia DI vystymuisi[260]. Nors paprastoje duomenų bazėje duomenų valdytojai gali nesudėtingai atrinkti atskiras asmenį identifikuojančios informacijos dalis ir jas panaikinti, problema kyla su asmens duomenimis, kurie yra didžiųjų duomenų rinkinio dalis – jų pašalinimas gali turėti įtakos DI tikslumui ir patikimumui. Pvz., kai DI algoritmai pereina mašininio mokymosi procesą, jie naudoja esamus duomenis specifinėms funkcijoms išmokti.[261] Panaikinus duomenų dalis, būsima algoritmų elgsena gali būti ne tokia, kokia būtų nepanaikinus duomenų, todėl algoritmų elgsena yra nestabili, mažiau patikima ir ne tokia tiksli. Dėl šios priežasties DI naudojami asmens duomenys, net ir juos panaikinus, neabejotinai gali likti integruoti kaip neuroninio tinklo dalis.[262] Taigi susiduriama su panašia problematika kaip anksčiau aptartu atveju, kai asmuo atšaukia sutikimą duomenų tvarkymui.

Be kita ko, teisės būti pamirštam įgyvendinimas gali kelti iššūkių ir įgyvendinant konkrečiai iš teisinės procedūrinės pusės kylančias pareigas. Kai duomenys, kuriuos prašoma ištrinti, yra viešojoje erdvėje, duomenų valdytojas privalo imtis pagrįstų priemonių, kad informuotų kitus duomenų valdytojus, jog duomenys ir bet kokie jų saitai ar kopijos turi būti ištrinti.[263] Praktikoje, vos vienam asmeniui pasinaudojus teise būti pamirštam ir reikalaujant ištrinti visas jo asmens duomenų kopijas, poveikis DI operacijoms gali išsitęsti per kelis lygius atskirų duomenų valdytojų.[264] Kitaip tariant, kreipimasis į vieną duomenų tvarkytoją dėl duomenų pašalinimo, duomenims nesant tiesiogiai tvarkomiems to vieno valdytojo, tokia užklausa užkabins eilę susijusių duomenų valdytojų. Šiame kontekste atkreiptinas dėmesys į vieną pastarųjų „Facebook“ sprendimų. „Facebook“ pristatė „Off-Facebook Activity“ įrankį, kuris pagal paskirtį neva leidžia vartotojams ištrinti jų duomenis, kuriais trečiųjų šalių programėlės ir svetainės pasidalijo su „Facebook“. Tačiau, kaip pažymima „MIT Technology Review“ – „*tai šiek tiek klaidina – Facebook nepanaikina jokių duomenų iš trečiųjų šalių, o tiesiog juos atsieja nuo savo*

[260] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 408 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[261] PARLOFF, R. *Why Deep Learning is Suddenly Changing Your Life*, FORTUNE, 2016, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://fortune.com/longform/ai-artificial-intelligence-deep-machine-learning/>.
[262] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 408 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[263] BDAR 17 str. 2 d.
[264] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 408 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.

turimų duomenų apie jus“.[265] Taigi informacijos ištrynimas kaip, iš principo, teisės būti pamirštam įgyvendinimo forma šiuo atveju apsiriboja tik poveikiu „Facebook“ asmeninių duomenų tvarkymui ir trečiųjų šalių, disponuojančių asmens duomenimis, atžvilgiu, neveikia. Toks sprendimas gali būti vertinamas kaip teisėtas teisės būti pamirštam kontekste „Facebook“ ribose, nes „Facebook“ algoritmai apdirbantys asmens duomenis atsieja tam tikrą apie asmenį per kitas programas surinktą informaciją, kai asmuo prie kitų programų būna prisijungęs su „Facebook“ paskyra. Tačiau duomenų apsaugos sąžiningumo principo prasme, vis dėl to kvestionuotina, ar sprendimas vidutiniškai išprususiam vartotojui yra pakankamai aiškus, nedviprasmiškas ir neleidžia manyti, jog asmuo ištrina savo duomenis plačiąja prasme.

Atkreiptinas dėmesys, jog pati teisė būti pamirštam yra kildinama iš panašaus atvejo byloje *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja González*[266] (toliau – **Costeja byla**). Byloje ESTT sprendė, kad interneto paieškos sistemos operatorius yra atsakingas už trečiųjų šalių paskelbtuose tinklalapiuose pateikiamos asmeninės informacijos tvarkymą. O pašalinimo pagrindais yra ne tik tai, jog duomenys yra netikslūs, bet ir tai, kad jie yra neadekvatūs, nereikšmingi ar pertekliniai pagal tvarkymo tikslus, neatnaujinti arba saugomi ilgiau, nei reikalinga, išskyrus atvejus, kai jie saugomi istoriniais, statistiniais ar moksliniais tikslais.[267] Jei paieškos sistema atmeta prašymą, asmuo gali kreiptis į atitinkamas institucijas svarstyti atvejį ir priėmus sprendimą paieškos sistemai gali būti nurodyta pašalinti nuorodas iš paieškos rezultatų[268]. Iš esmės šioje byloje teismas išaiškino, jog teisė būti pamirštam interneto paieškos rezultatuose yra viršesnė už paieškos variklio eksploatuotojo ekonominį interesą ir už visuomenės interesą

[265] JEE, C. *Facebook has finally launched its “clear history” button … but it doesn’t delete anything*, Silicon Valley, MIT Technology Review, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.technologyreview.com/f/615111/facebook-has-finally-launched-its-clear-history-button-but-it-doesnt-delete-anything/>.

[266] Europos Sąjungos Teisingumo Teismas. *2014 m. gegužės 13 d. sprendimas Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González C-131/12, EU:C:2014:317.*

[267] *Ibid.* žr. 72 ir 92 p.

[268] Pažymėtina, jog vėlesniame sprendime Google LLC, Google Inc. teisių perėmėja, prieš Commission nationale de l’informatique et des libertés (CNIL), ESTT sprendė, kad paieškos sistemos operatorius, atlikdamas RTBF prašymą, neprivalo atlikti nuorodų pašalinimo globaliu mastu. Tačiau reikalaujama panaikinti nuorodas į jo paieškos sistemos versijas pritaikytas visoms valstybėms narėms, ir imtis priemonių pagrindinėms duomenų subjekto teisėms apsaugoti. Žr. Europos Sąjungos Teisingumo Teismas. *2019 m. rugsėjo 24 d. sprendimas Google LLC prieš Commission nationale de l'informatique et des libertés (CNIL) C-507/17, EU:C:2019:772.*

turėti prieigą prie šios informacijos.[269] Po 2014 m. ESTT sprendimo Costeja byloje[270], duomenų subjektas gali prašyti internetinės paieškos sistemos teikėjo ištrinti vieną ar kelias nuorodas į tinklalapius iš rezultatų sąrašo, rodomo atlikus paiešką pagal jo vardą ir pavardę. Sprendimas buvo eskaluotas kaip „teisės būti pamirštam sprendimas“, nors ESTT pažodžiui ir neužtikrino tokios teisės. Teismas argumentavo remiantis duomenų subjekto teisėmis, kylančiomis iš Chartijos 7 str. (pagarba privačiam ir šeimos gyvenimui) ir 8 str. (asmens duomenų apsauga).[271]

Taigi teisės būti pamirštam įgyvendinimas iš tiesų kelia daug probleminių klausimų. Turint omenyje, jog informacijos pamiršimo realus įgyvendinimas aktualiu metu, galima vertinti, jog yra dar tik sprendžiamas, iš DI perspektyvos šios teisės įgyvendinimas kvestionuotina, ar kol kas išvis nėra fikcija.

3.2.2 Teisė į duomenų perkeliamumą

Teisė į duomenų perkeliamumą – viena iš BDAR naujai suformuluotų duomenų subjekto teisių.[272] Teisės į duomenų perkeliamumą tikslas – geresnė asmens duomenų kontrolė, pagerinant duomenų subjektų galimybes lengvai perkelti, kopijuoti ir perduoti savo duomenis iš vienos informacinių technologijų aplinkos į kitą. Viena vertus, iš pozityviosios pusės taip palengvinama vieno paslaugos teikėjo keitimas kitu, paskatinama jų konkurencija ir naujų paslaugų kūrimas,[273] be to, informacijos platinimo sąlygų supaprastinimas palengvina mažesniems duomenų valdytojams reikalingas pastangas rinkti

[269] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 186.

[270] Europos Sąjungos Teisingumo Teismas. *2014 m. gegužės 13 d. sprendimas Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González C-131/12, EU:C:2014:317.*

[271] Pažymėtina, jog po ESTT sprendimo Costeja byloje, priežiūros institucijos pastebėjo, kad padaugėjo skundų dėl paieškos sistemų valdytojų atsisakymo panaikinti nuorodas iš rezultatų. To pasekoje ES imtasi priemonių šiame kontekste sprendžiant reguliavimo spragas ir siekiant įstatymo raidės aiškumo. EDAV, siekiant išaiškinti teisę būti pamirštam paieškos sistemų atvejais pagal BDAR nuostatas, išleido viešą konsultaciją dėl gairių dėl teisės būti pamirštam būtent paieškos sistemų atvejais pagal BDAR (žr. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201905_rtbfsearchengines_forpublic consultation.pdf>). Vertintina, jog visuomenės suinteresuotumas ir reguliavimo aiškumo poreikis nemažta. Visgi kol šios gairės nebus baigtos, priežiūros institucijos turi ir toliau, kiek įmanoma, laiku nagrinėti ir tirti duomenų subjektų skundus.

[272] BDAR 20 str. 1 d.

[273] 2017 m. balandžio 5 d. Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, WP 242 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.

duomenis.[274] Kita vertus, iš šios teisės kylančios pareigos duomenų valdytojams, investuojantiems į aukšto lygio technologijas duomenims apdirbti, vertinama, jog yra iš esmės nepalankios.

Teisė į perkeliamumą reikalauja, kad duomenų valdytojai palaikytų procesus, skirtus identifikuoti ir izoliuoti asmens tapatybę identifikuojančią informaciją.[275] Tokių procesų užtikrinimas, taip pat kaip ir reikalavimas duomenų subjektui pateikti struktūruotą ataskaitą, techniškai nėra itin sofistikuotos užduotys. Šiuo atveju pats duomenų perdavimas kitam duomenų valdytojui yra nenaudinga konkurencijos rinkoje atžvilgiu: tokiu būdu duomenų valdytojai atsisako konkurencinių pranašumų.[276] Nežiūrint to, kokia ankstesnio duomenų valdytojo pasitelkiama technologija ar sąnaudomis duomenys buvo renkami ir kategorizuojami – jie gali būti struktūruotai vienu veiksmu perduodami konkurentams didžiuosius duomenis apdirbančiųjų rinkoje. Pažymėtina, jog DI technologijos vystymasis pagal dabartinį modelį ir priklauso nuo didelio duomenų kiekio rinkimo; dideli duomenų rinkiniai suteikia išskirtinį konkurencinį pranašumą.[277] Tai iš esmės sukuria disbalansą tarp pirminių duomenų tvarkytojų investuojančių į duomenų apdirbimo technologijas ir antrinių duomenų subjektų, kurie gavę subjekto išsineštus duomenis įsisavina duomenis be jokių specifinių kaštų.

Taigi, teisės į duomenų perkeliamumą ypatumas DI atžvilgiu nekelia specifinių teisinių ar techninių problemų, tačiau iš verslo pusės nėra naudingas tarpusavyje rinkoje konkuruojantiems duomenų valdytojams. Tai vertintina kaip atspindys atvejų, kuomet įgyvendinant įstatymų leidėjo tikslus gali būti sukuriama tam tikra disproporcija tarp siekio užtikrinti silpnesniosios šalies teises ir stambesnių *žaidėjų* privačius, pelno siekimo, tačiau teisėtus interesus.

[274] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 409 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[275] 2017 m. balandžio 5 d. Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, WP 242 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.
[276] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018, p. 409 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[277] *Ibid.*

3.2.3 Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą

Įprastam profiliavimui ir automatizuotam sprendimų priėmimui, kurio rezultate žmogus priima galutinį sprendimą, kokiu būdu DI paprastai ir yra naudojamas, taikomos įprastos BDAR nuostatos dėl asmens duomenų tvarkymo. Tačiau kalbant apie visiškai autonominį automatizuotą atskirų sprendimų priėmimą, įskaitant profiliavimą, reglamente numatytas itin griežtas reguliavimas.[278] Šioje darbo dalyje skirtinas ypatingas dėmesys pastarajam atvejui – įtvirtintam BDAR 22 str.

BDAR pirmtakės – Duomenų apsaugos direktyvos – 15 str. fiziniams asmenims suteikė teisę į tai, kad jiems nebūtų taikomi visiškai automatizuoti, profiliavimu (nebūtinai) pagrįsti sprendimai. Nors ši teisė buvo novatoriška ir intriguojanti, per visą jų gyvavimo laikotarpį pagal Duomenų apsaugos direktyvą ji nebuvo praktiškai įgyvendinta.[279] Jos esmę su tam tikrais pakeitimais atkūrė ES BDAR. Ši teisė papildoma naujomis atskleidimo pareigomis, taikomomis duomenų valdytojams, vykdantiems visiškai automatizuotą sprendimų priėmimą.[280]

BDAR numatytas specialusis autonominio automatizuoto atskirų sprendimų priėmimo ir profiliavimo apribojimas yra vienas iš didžiausią reikšmę DI turinčių BDAR suformuluotų taisyklių. Pagal bendrą nuostatą duomenų subjektui suteikiama teisė, kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį.[281] Praktikoje toks asmens duomenų tvarkymas gali būti atliekamas siekiant įvertinti tam tikrus su duomenų subjektu susijusius asmeninius aspektus, pvz., jo veiklą darbe, kreditingumą, patikimumą, elgesį ir kt. Taip tvarkant duomenis taikomi visi bendrieji reikalavimai tiek, kiek specialieji reikalavimai nenumato kitaip.[282]

Vertinant 22 str. ginamos duomenų subjekto teisės ir iš to kylančių reikalavimų automatizuotam atskirų sprendimų priėmimui, įskaitant profiliavimą, reguliavimą, pirmiausia pažymėtina atskirties tarp pačių automatizuoto sprendimų priėmimo ir

[278] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 258-261.
[279] *Ibid*. p. 248.
[280] BDAR 13 str. 2 d. f p. ir 14 str. 2 d. g p.
[281] *Ibid.* 22 str. 1 d.
[282] ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019, p. 249.

profiliavimo koncepcijų aspektai, tuomet pačios BDAR normos *rationale* ir taikymo DI ypatumai.

3.2.3.1 Automatizuotas atskirų sprendimų priėmimas v. profiliavimas: kategorijų skirtis

Pagal įstatymų leidėjo tiesiogiai arba netiesioginiai *ad legem* įtvirtintus apibrėžimus, automatizuotą sprendimų priėmimą ir profiliavimą autonominio sprendimų priėmimo kontekste galima skirti pagal tokius sudėties elementus:

- aiškinant BDAR 71 konst. d. p. automatizuotas sprendimų priėmimas yra: (I) procesas, kurio metu (II) taikant tam tikras technologijas (III) sprendimai priimami (IV) be žmogaus įsikišimo. (V) Šie sprendimai gali būti grindžiami: (i) faktiniais duomenimis, taip pat (ii) skaitmeniniu būdu sukurtais profiliais arba (iii) numanomais duomenimis.
- Kuomet profiliavimas, kurio sąvoka jau konkrečiai apibrėžiama BDAR 4 str. 4 p., yra: (I) bet kokios formos automatizuotas duomenų tvarkymas, (II) naudojant asmens duomenis ir (III) siekiant įvertinti su fiziniu asmeniu susijusius asmeninius dalykus. BDAR nuostata šiuo atveju grindžiama Europos Tarybos rekomendacijoje[283] pateikta profiliavimo apibrėžtimi, tačiau ji nėra identiška, nes rekomendacijoje neįtraukiama duomenų tvarkymas, kuriuo neprieinama išvadų.[284]

Atitinkamas skaidymas leidžia įvertinti, ar kiekvienu atveju praktinė situacija atitinka vieną iš reglamento kategorijų. Visgi, pats skirtumas tarp jų geriau atsiskleidžia vertinant pačią procesų paskirtį:

- automatizuotas sprendimų priėmimas *per se* nėra susijęs su asmeninių savybių analize ir pagal tikslą yra orientuotas į sprendimo priėmimą automatizuotu, autonominiu būdu;
- kuomet profiliavimui – algoritmai naudojami siekiant surasti koreliacijas tarp atskirų duomenų rinkinių ir įvertinti asmeninius individo aspektus, net jei joks sprendimas rezultate ir nėra priimamas. Profiliavimas turi apimti tam tikrą automatinio apdorojimo formą, nors žmogaus dalyvavimas nebūtinai išbraukia

[283] 2010 m. lapkričio 23 d. Council of Europe, the Protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://rm.coe.int/16807096c3>.
[284] Vis dėlto rekomendacijoje naudingai išdėstoma, kad profiliavimas gali apimti tris atskirus etapus: (i) duomenų rinkimas; (ii) automatizuota koreliacijų nustatymo analizė; (iii) koreliacijos asmeniui pritaikymas esamam ar būsimam elgesiui identifikuoti. Profiliavimą vykdantys kontrolieriai turės užtikrinti, kad jie atitiktų visų pirmiau nurodytų etapų BDAR reikalavimus.

veiklą iš apibrėžimo.[285] Gali būti naudojami trys profiliavimo būdai: (i) bendras klasifikavimas; (ii) sprendimų priėmimas remiantis profiliavimu; (iii) tik automatizuotas sprendimų priėmimas, įskaitant profiliavimą, kuris daro teisinį poveikį arba panašiai daro didelę įtaką duomenų subjektui (papuola po 22 str.).[286]

Taigi kategorijos gali būti naudojamos visiškai atskirai, tačiau gali ir dubliuoti ar papildyti viena kitą. Automatizuotas sprendimų priėmimas gali iš dalies persidengti su profiliavimu arba būti profiliavimo rezultatas, gali vykti ir visai be profiliavimo – lygiai taip ir profiliavimas – gali nebūti finalizuojamas automatizuoto sprendimų priėmimo. Visgi anot Brkan, daugelis, jei ne dauguma bendrame 22 str. nustatytų sprendimų, tikėtina, apims profiliavimą[287].

3.2.3.2 Normos *rationale*

Įvertinus abiejų 22 str. dedamųjų skirtį, suderinamumą duomenų tvarkymo procesuose ir paskirtį, galima konstruktyviau vertinti bendrą normos tikslą. Pačioje BDAR preambulės 71 konst. d. pabrėžiamas susirūpinimas dėl galimų klaidų ir nesąžiningos diskriminacijos rizikos, susijusios su automatizuotu sprendimų priėmimu ir profiliavimu. Kadangi tokie sprendimai gali būti ir didelės reikšmės arba turėti teisinį poveikį, sprendžiama, jog juos turėtų priimti kiti vis dar *žmogiško prado* asmenys, galintys atsižvelgti į konkrečias asmeniui susiklosčiusias aplinkybes. Taigi, bendrai vertinant, numatyta duomenų subjekto teisė suformuluota siekiant įveikti IT plėtros poveikį, dėl kurio vis dažniau sprendimai priimami mechaniškai.

Visgi normos pagrindas suponuoja atskirą klausimą dėl pačios straipsnio 1 d. numatytos teisės veikimo: ar (i) ji nustato teisę, kuria duomenų subjektas gali naudotis, autonomiškai disponuoja galimybe ja pasinaudoti ar (ii) iš tikrųjų nustato kvalifikuotą tam tikro tipo sprendimų priėmimo proceso draudimą, neatsižvelgiant į duomenų subjekto prieštaravimus? Jau nagrinėjant DPD įgyvendinimą, tai buvo vienas didžiausių Korff nurodytų probleminių klausimų[288]. Pagal BDAR 22 str. iš pirmo žvilgsnio klausimas atrodo

[285] 2018 m. vasario 6 d. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, p. 7 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.
[286] *Ibid*. 8 psl.
[287] BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology,* 2019 DOI; 10.1093/ijlit/eay01, p. 97 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.
[288] KORFF, D. EC Study on Implementation of Data Protection Directive 95/46/EC [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667>.

išspręstas – nuostata aiškiai suformuluota kaip teisė, ir priskirta prie duomenų subjekto teisių skyriaus BDAR. Visgi vertinimo pozicijos teisės moksle ir šiuo atveju išsiskiria. Vieni autoriai ją laiko teise, nes tai:

1. atitinka tikrąją jo formuluotę ir yra prasminga atsižvelgiant į kitas BDAR nuostatas, kurios leidžia manyti, kad jau egzistuoja pagal taisykles nustatyti sprendimų priėmimo procesai.[289]
2. Tai pripažintų, kad šie sprendimų priėmimo procesai jau plačiai naudojami tiek privačiuose, tiek valstybiniuose sektoriuose, kur skaitmeninimas yra pažangus.
3. Geriau pateisintų tai, kad šie sprendimų priėmimo procesai gali turėti socialiai pateisinamos naudos (ne tik galimos naudos).[290]

Kiti – draudimo forma[291], nes:

1. Tai suteikia jam daugiau kandumo ir taip labiau pateisina reglamento tikslą stiprinti duomenų apsaugą.
2. Išsaugomas 22 str. 3 d.[292] numatytas „žmogaus dalyvavimo“ apsaugos funkcionalumas ir BDAR suderinamas su Teisėsaugos duomenų apsaugos direktyvos[293] formuluote, todėl ES duomenų apsaugos sistema tampa nuoseklesnė[294].
3. 29 str. darbo grupė šiuo atveju pažymi, jog – „jei 22 str. aiškintume kaip suteikiantį teisę nesutikti, 22 str. 2 d. c p. nustatyta išimtis nebūtų labai prasminga. Pagal šią išimtį, automatizuotas sprendimų priėmimas gali būti vykdomas, jei duomenų subjektas duoda aiškų sutikimą <...>. Tokiu atveju kiltų prieštaravimų, nes

[289] BDAR 13 str. 2 d. f p.
[290] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 252-253.
[291] Žr. pvz. BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.
[292] BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.
[293] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR *OL L 119, 2016 5 4.*
[294] BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01, p. 99 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

duomenų subjektas negali pareikšti ir nesutikimo, ir sutikimo dėl to paties duomenų tvarkymo.“[295]

Nors pozicijos išsiskiria, autorės manymu, DI sistemų atžvilgiu dėl 29 str. darbo grupės pozicijos autoritetingumo derėtų laikytis šios aiškinimo politikos ir vertinti automatizuoto sprendimų priėmimo įskaitant profiliavimą reikalavimus kaip savaime galiojantį suformuluotą draudimą duomenų tvarkymo procedūrų atžvilgiu.

3.2.3.3 Normos taikymas dirbtiniam intelektui

BDAR 22 str. pirminiu vertinimu, kaip ir būdinga visam BDAR, išlieka technologiškai neutralus sutelkiant dėmesį ne į technologiją, kuri priima automatizuotą sprendimą, o į patį sprendimą ir jo automatizuotą priėmimo procesą[296]. Nepaisant to, akivaizdu, kad ši nuostata iš esmės (nors ir ne išskirtinai) skirta programoms, kurios, pagal intelekto laipsnį, dažniau priskirtinos robotams ir (arba) DI. Be to, straipsnis apima profiliavimą, kuris rodo, kad programa yra pažangesnė, nes dažnai (nors ne visada) apima didžiųjų duomenų analizę arba kitus sudėtingus metodus, reikalaujančius aukštesnio programos intelekto lygio.[297]

Vertinant patį straipsnio objektą, straipsnis konkrečiai apima ne visus DI sprendimus. Taikymo apimtis yra tiksli ir gana siaura:

1. Sprendimas turi būti grindžiamas „tik“ automatizuotu duomenų tvarkymu;
2. Sprendimas turi turėti teisinį arba panašų reikšmingą poveikį duomenų subjektui. Teisinis poveikis yra gana aiškus, o dėl reikšmingo poveikio traktavimo praktikoje kyla neapibrėžtumo problematika. Visgi EDAV siūloma, jog į šią kategoriją galėtų būti įtraukti sprendimai, kurie turi įtakos žmogaus finansinei padėčiai, pvz., jo teisei gauti kreditą; turintys įtakos asmens galimybėms naudotis sveikatos priežiūros paslaugomis; sprendimai, dėl kurių asmeniui nesuteikiama galimybė įsidarbinti arba jis atsiduria labai nepalankioje padėtyje; sprendimai, turintys įtakos asmens galimybėms gauti išsilavinimą, pvz., priėmimas į universitetus.[298]

---

[295] 2018 m. vasario 6 d. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053> 38 psl.

[296] BDAR 22 str. 1 d.

[297] WRIGLEY, S., BOTS, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199, 2019, p. 204-208 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą:
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>.

[298] 2018 m. vasario 6 d. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01, 22 psl. [interaktyvus.

Kaip Korff vertino BDAR 22 str. DPD pirmtakę nuostatą – „apskritai ši nuostata taikoma labai retai,[299] DI sprendimų, kuriems taikoma ši BDAR nuostata, skaičius taip pat gali būti pakankamai nedidelis. Daugeliu atvejų duomenų valdytojams gali būti gana lengva priimti sprendimą už nuostatos taikymo srities ribų, įtraukiant į procesą žmogaus sprendimus priimantį asmenį.[300] Straipsnyje nustatytų reikalavimų taikymą praktiškai apsunkina ir tai, jog norma taikymo prasme visapusiškai apsunkinta išimtimis. Anot Bygrave, kortų namelio metafora, naudojama jos pirmtakei normai DPD apibūdinti[301], jai tinka vienodai gerai – trūksta visai nedaug, jog būtų netaikytina.

Pirmiausia straipsnio 2 d. numato 3 išimtis, kuomet 1 d. įtvirtinta teisė neegzistuoja: (i) sutartis, (ii) įstatymo pagrindas arba (iii) sutikimas. Anot Sam Wrigley, duomenų valdytojams gana lengva naudoti vieną iš 2 d. pateiktų išimčių – nemaža tikimybė, kad duomenų subjektai sutiks tvarkyti tinkamai neperskaitę pranešimo apie privatumą. Be to, galima tikėtis, kad daugeliu atvejų, kai sprendimas turės atitinkamą reikiamą poveikį duomenų subjektui, duomenų tvarkymą atliks oficiali institucija įstatymo pagrindu arba šalys palaikys sutartinius santykius. Todėl galima daryti prielaidą, kad valdytojai paprastai galės be per didelių sunkumų naudotis automatizuotu sprendimų priėmimu.[302]

Antro lygio išimtys nurodytos straipsnio 3 dalyje, kurioje teigiama, kad, neatsižvelgiant į 2 dalyje numatytas sutarties ir sutikimo išimtis, esti jų atžvilgiu „bent“ dar trys duomenų subjekto teisės:[303] (i) teisė iš duomenų valdytojo reikalauti žmogaus įsikišimo, (ii) teisė pareikšti savo požiūrį ir (iii) teisė užginčyti sprendimą. Teisinėje bendruomenėje ginčijama, kokios kitos teisės apimamos,[304] ypač sprendžiama, ar duomenų

Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

[299] KORFF, D. EC Study on Implementation of Data Protection Directive 95/46/EC, p. 115 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667>.

[300] WRIGLEY, S., BOTS, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199 (2019) [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>, p. 204-208.

[301] BYGRAVE, L. A. *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law & Security Review 17(1):17-24, 2001, p. 21 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/220668128_Data_Protection_Law_Approaching_its_Rationale_Logic_and_Limits_by_L_A_Bygrave>.

[302] WRIGLEY, S., BOTS, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>, p. 204-208.

[303] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 251-255.

[304] *Ibid*. p. 254-255.

subjektams turi būti suteikta teisė *ex post* paaiškinti jiems įtaką darančius automatizuotus sprendimus. Vyrauja dvi nuomonės:

1. Nors BDAR preambulėje aiškiai minima tokia teisė[305], reglamento rezoliucinės nuostatos negalioja, todėl bent jau teisiškai įgyvendintina forma teisės pagal reglamentą nėra;[306]
2. Kiti mokslininkai nesutinka[307], nes:
    i. Ši teisė egzistuoja ir kitose BDAR nuostatose suteikiančiose teisę į „prasmingą informaciją apie loginį jo [automatizuoto sprendimo] pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui.“[308]
    ii. Teisė į *ex post* paaiškinimą užtikrina kitų BDAR teisių, pvz., teisės užginčyti sprendimą[309] veiksmingumą ir pažeidžia bendrąjį BDAR reikalavimą asmens duomenis tvarkyti sąžiningai ir skaidriai[310].
    iii. Teisė į *ex post* paaiškinimą neabejotinai kyla iš bendrųjų BDAR nustatytų duomenų valdytojų atskaitomybės reikalavimų[311].

Galiausiai, straipsnio 4 dalis taip pat numato tam tikrą sąlyginį straipsnio taikymą – turi būti taikomi papildomi tvarkymo apribojimai, kai sprendimas grindžiamas ypač jautriais asmens duomenimis. Tai yra BDAR naujovė. Taip pat ir vaikų, kaip duomenų subjektų, apsauga niekada nebuvo aiškiai aptariama DPD, tačiau ji užima svarbią poziciją BDAR, įskaitant ir profiliavimo srityje - „ypatinga apsauga visų pirma turėtų būti vaikų asmens duomenų naudojimui rinkodaros, virtualios asmenybės ar vartotojo profilio

[305] BDAR 71 konst. d.: „*Bet kuriuo atveju tokiam duomenų tvarkymui turėtų būti taikomos tinkamos apsaugos priemonės, įskaitant konkrečios informacijos duomenų subjektui suteikimą ir teisę reikalauti žmogaus įsikišimo, pareikšti savo požiūrį, gauti sprendimo, priimto atlikus šį vertinimą, paaiškinimą ir teisę ginčyti tą sprendimą*.“

[306] WACHTER, S. et al. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469>.

[307] pvz. BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

[308] BDAR 13 str. 2 d. f p., 14 str. 2 d. f p., 15 str. 1 d. h p.

[309] *Ibid*. 22 str. 3 d.; BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01, p. 114 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

[310] BDAR 5 str. 1 d. a p.

[311] *Ibid*. 5 str. 2 d. ir 24 str.; BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 254-255.

sukūrimo tikslais ir su vaikais susijusių asmens duomenų rinkimui naudojantis vaikui tiesiogiai pasiūlytomis paslaugomis“[312], o priemonė, susijusi su automatizuotu sprendimu, grindžiama profiliavimu „negali būti susijusi su vaiku“[313].

Be išimčių taikymo, nagrinėjant normos taikymo DI ypatumus, būtina atsižvelgti ir į tai, jog apsaugos lygis pagal 22 str. papildomai priklausys ir nuo valstybių narių teisės aktų specifikos. Atsižvelgiant į 22 str. 2 d. b p. ir 22 str. 4 d. numatytas nukrypti leidžiančias nuostatas ES valstybėms narėms šiuo atžvilgiu suteikta gana plati diskrecija, todėl gali atsirasti nemažų automatizuoto sprendimų priėmimo nacionalinių reguliavimų skirtumų. Visgi žingsnį, kol kas, žengė dar nedaug valstybių narių.[314] Nepaisant galimai išryškėsiančių skirtumų potencialo, galima tikėtis, kad nacionalinių teisės aktų leidėjai visoje Europoje priims ir gana panašius sprendimus dėl tam tikrų klausimų rinkinių, pvz. susijusių su vaikų apsauga[315]. Nors BDAR konstatuojamosios dalys savaime nekuria teisiškai privalomo automatizuotų sprendimų ar profiliavimo, skirtų vaikams, draudimo, tikėtina, kad jos paskatins nacionalinių aktų griežtinimą, kuris 22 str. nuostatos atžvilgiu bus taikomos nacionaliniu lygmeniu.[316] Iš duomenų valdytojų pusės tokiu būdu reikalavimai DI sistemų projektavimui ir priežiūrai ribojant autonomiją dar griežtėtų.

Sutiktina su Lee A. Bygrave, jog pakankamai paini 22 str. struktūra neskatina aiškumo ir supratimo apie jo svarbą, ypač *mėgėjams*.[317] Todėl DI tvarkančio duomenis atžvilgiu svarbus duomenų valdytojo indėlis užtikrinti, kad duomenų apie asmenis tvarkymo alternatyvūs teisiniai pagrindai kiekvienu atveju sutiktų su straipsnio keliama pagrindine asmens teise (ar draudimu), atitinkamai įvertinant nurodytas kelių lygių išimtis. Turint omenyje DI sistemas pačias pagal poreikį gebančias inicijuoti duomenų rinkimą ir apdirbimą skirtingose situacijose, toks kiekvieno atvejo klasifikavimas pagal straipsnyje keliamus reikalavimus turėtų būti atsakingai įdiegiamas jau algoritmų kūrimo fazėje.

Be kita ko, analizuojant normos taikymo ypatumus DI, atkreiptinas dėmesys, kad įstatymų leidėjo sulaukta daug įvairios kritikos ir dėl šios įtvirtintos teisės praktinio taikymo ir poveikio DI. Pastebima, jog dažnu atveju pozicijos formuojamos gana

[312] BDAR 38 konst. d. p.
[313] *Ibid*. 71 konst. d. p.; BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 251-255.
[314] *Ibid*.
[315] BDAR 71 ir 38 konst. d. p.
[316] *Ibid.* pvz., aiškinant, kokie sprendimai gali būti laikomi turinčiais *reikšmingą* poveikį (22 str. 1 d.).
[317] BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019, p. 251-255.

kategoriškai, pagal ką galima netiesiogiai įžvelgti technologijų ir duomenų apsaugos šalininkų interesų konfrontaciją.

Literatūroje vienų vertinama, jog apsauga nuo asmenų profiliavimo šalina DI komercinį naudingumą ir jo gebėjimą mokytis. Siekiant veiksmingumo, dauguma komercinio DI naudojimo vartotojų atžvilgiu remiasi analize ir prognozėmis, pagrįstomis unikaliomis asmens savybėmis.[318] Tačiau pagal BDAR asmenys gali prieštarauti duomenų tvarkymui, naudojamam „analizuoti ar prognozuoti aspektus, susijusius su to fizinio asmens veikla darbe, ekonomine padėtimi, sveikata, asmeninėmis nuostatomis, interesais, patikimumu, elgesiu, vieta ar judėjimu“.[319] Apribodamas klasifikavimą, DI negali mokytis iš žmogaus, grupės ar individualaus elgesio ir gali būti neperspektyvus plataus naudojimo veiklai. Be to, teisė prieštarauti aiškiai apeliuoja ir į tiesioginę rinkodarą, rinkodaros taktiką, pagal kurią individualus pirkėjo elgesys naudojamas ateities tikslams prognozuoti, kad reklama būtų pritaikyta konkrečiam asmeniui, kaip prieštaringas apdorojimo tikslas.[320] Be to pažymima, jog, praktine prasme, organizacijoms, kurios naudoja DI, yra praktiška naudoti neprižiūrimus mašininio mokymosi modelius. Nors prižiūrimas mokymosi modelis algoritmams kurti naudoja pažymėtus duomenų rinkinius, papildytus žmonių priežiūra, neprižiūrimi modeliai leidžia DI vystytis savarankiškai.[321] Su neprižiūrimais modeliais gali būti neįmanoma atsekti DI mokymosi procesų arba paaiškinti savo sprendimų, nes trūksta duomenų žymių ir ryšių. Net prižiūrimus modelius atskirais atvejais gali būti per sunku paaiškinti, o tai pakenktų vienam naudingiausių DI tikslų – automatizuotiems sprendimams ir prognozėms.[322] Todėl šiuo atveju Matthew Humerick vertina, jog BDAR duomenų privatumo teisių apsauga riboja naudingiausių DI funkcijų – autonomijos ir

[318] Žr. pvz. KAPUT, M. *How Brands Target Consumers Better and Sell More with Artificial Intelligence [Case Studies Included]*, Marketing AI Institute, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.marketingaiinstitute.com/blog/how-brands-target-consumers-better-and-sell-more-with-artificial-intelligence-case-studies-included>.
[319] BDAR 4 str. 4 d., 21 str.
[320] *Ibid*. 21 str. 2-3 d.
[321] Žr. SONI, D. *Understanding the Different Types of Machine Learning Models*, Towards Data Science, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://towardsdatascience.com/understanding-the-different-types-of-machine-learning-models-9c47350bb68a>.
[322] Taip yra todėl, kad algoritmas gali pastebėti koreliaciją, bet negali paaiškinti ryšio, nes negali suprasti prasmės, kaip žmogus gali žr. pvz., WALLACE, N. EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence, TECHZONE360, 2017, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm>.

automatizavimo – naudojimą. Iš komercinės pusės DI pritaikymas yra iš esmės pagal BDAR ribojamas, dėl ko verslas gali atsisakyti būsimų investicijų į šią technologiją[323].

Kiti pažymi, kad galutinė priežastis, nuvertinti 22 str. svarbą, yra ta, kad daugeliui jame išdėstomų apsaugos priemonių jau taikomi bendrieji BDAR principai. Kaip pažymėjo JK informacijos komisaro tarnyba, duomenų tvarkymas visada turi būti sąžiningas pagal duomenų tvarkymo principus[324], todėl kai kurie 22 str. numatyti apsaugos reikalavimai kartais pertekliniai. Todėl 22 str. nustatyti reikalavimai dėl tam tikrų apsaugos priemonių nebūtinai suteikia daugiau apsaugos.[325]

Taigi visiškai autonominio automatizuotų sprendimų priėmimo, įskaitant profiliavimą, kaip tai suprantama pagal 22 str. sudėties elementus, draudimas yra bene griežčiausias BDAR reguliavimo aspektas, nubrėžiantis teisėtai realizuotinam DI potencialui tikslias ribas. Silpnesniu įstatymų leidėjo paliktu aspektu, atviru įrodinėjimui ir teismų praktikai apspręsti būtų galima laikyti priimamo sprendimo poveikio masto duomenų subjektui vertinimą. Tai palieka galimybę duomenų valdytojams gintis nuo atsakomybės ir *vice versa* savo teises ginti duomenų subjektams. Antra vertus, ir numatytos straipsnio taikymo išimtys gali tapti sprendimu ir galimybe išvengti šio itin griežto reguliavimo. Tokiu būdu, pvz. asmenims davus sutikimą, kas, kaip aptarta, praktikoje yra dažnai atliekama per daug neįsigilinus, *kelias atviras* įprastam autonominio automatizuoto sprendimų priėmimo vykdymui duomenų apsaugos normų ribose. Visa tai įvertinus akivaizdu, kodėl dėl šios normos ypatingos svarbos, literatūroje ir plačiojoje visuomenėje gausu įvairių pozicijų nagrinėjančių jos poveikį technologijų aplinkai. Visgi, šiuo metu padaryti tvirtą ir galutinę išvadą dėl jos įtvirtinimo kokybės, pagrįstumo ir taikymo peripetijų yra sudėtinga – dar stingama praktikos kaip norma bus įgyvendinama, o tai priklausys tiek nuo galimos papildomos nacionalinės teisėkūros, tiek svarbus vaidmuo teks teismų, ypač ESTT praktikai.

[323] HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
[324] KORFF, D. EC Study on Implementation of Data Protection Directive 95/46/EC, p. 116 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667>.
[325] WRIGLEY, S., BOTS, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199, 2019, p. 204-208 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą:
<https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>.

IŠVADOS

1. DI technologija masiškai naudoja informaciją apie konkrečius asmenis, todėl kyla pavojus asmenų teisei į privatumą ir duomenų apsaugą. Asmens duomenų apsaugos reguliavimu siekiama apsaugoti šias vertybes ir užtikrinti saugią DI technologijų plėtrą. Kadangi duomenys yra DI mokymosi pagrindas – DI vystymosi galimybės yra neatsiejamos nuo reguliavimo aplinkos.
2. Tiek ES, tiek JAV aktyviai leidžiami DI strategiją formuojantys aktai. Nors ES laikytina pasaulio lydere technologijų reguliavime asmens duomenų apsaugos srityje, reguliavimas pradedamas griežtinti ir JAV. Lietuvoje atskirų duomenų apsaugos reguliavimo priemonių DI kontekste nesiimta, sprendimai DI srityje apsiriboja išleista DI strategija bei pasirašyta tarpvyriausybine deklaracija.
3. Pamatinis DI reguliavimo iššūkis yra tai, jog nėra vieningo teisinio DI apibrėžimo. Problematikos ES išvengiama į principus orientuotu ir technologiškai neutraliu BDAR reguliavimu, lemiančiu pritaikomumą įvairioms technologijoms ilgalaikėje perspektyvoje.
4. BDAR yra pagrindinė teisinė priemonė ES, nustatanti duomenų apsaugos taisykles taikytinas DI. Visgi, BDAR reguliavimas taikomas ne tik ES, tačiau ir bet kurioje pasaulio valstybėje įsisteigusiems DI pasitelkiantiems subjektams, jei duomenų tvarkymo veikla orientuojama į ES esančius duomenų subjektus. Vis dėlto BDAR yra taikomas tik tuomet, kai DI tvarko asmens duomenis, kaip jie apibrėžti BDAR.
5. BDAR teisėtumo, sąžiningumo ir skaidrumo principas yra fundamentalus pagrindas DI asmens duomenų tvarkymo veiklos atitikčiai duomenų apsaugos reikalavimams vertinti.
6. Dėl sudėtingų DI veikimo pricipų, objektyvus ir sąmoningas duomenų subjekto sutikimas dėl asmens duomenų tvarkymo galimas tik užtikrinus DI duomenų tvarkymo procesų praktinį paaiškinamumą. Vien procedūrinis BDAR reikalavimų laikymasis gali vesti prie beprasmio skaidrumo ir beprasmio sutikimo praktikoje.
7. BDAR duomenų kiekio mažinimo ir duomenų tvarkymo tikslo apribojimo principai bei duomenų subjekto teisės atšaukti sutikimą ir teisės būti pamirštam užtikrinimas vertintini kaip išskirtinai ribojantys savarankiško DI vystymosi galimybes, nes išbalansuoja giliojo mokymosi procesus bei mažina DI prieinamų rezultatų tikslumą.
8. BDAR užtikrinta duomenų subjekto teisė į duomenų perkeliamumą mažina duomenų valdytojų, investuojančių į DI, konkurencinį pranašumą, suteikiant galimybę kitiems duomenų valdytojams perimti surinktus duomenis išvengiant investicijų į juos renkančias sistemas.

9. Reikšmingiausios DI atliekamam asmens duomenų tvarkymui yra pritaikytosios ir standartizuotosios duomenų apsaugos bei automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą, BDAR nuostatos. Pritaikytosios ir standartizuotosios duomenų apsaugos principas svarbus kaip pažymintis standartizuoto asmens duomenų tvarkymo apimties principines ribas ir esminius reikalavimus DI pasitelkiančiam subjektui tinkamoms techninėms ir organizacinėms priemonėms užtikrinti. Kuomet automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą, ribojimas, išskirtinas kaip kertinis BDAR saugiklis nubrėžiantis tikslias ribas DI potencialui – uždraudžiama bet kokia DI autonomija savarankiškai priimti teisinius ar kitus didelio poveikio sprendimus.
10. Nors tiek etikos klausimai, tiek strateginiai DI reguliavimo orientyrai apspręsti nemažoje apimtyje įvairaus pobūdžio aktų, o imperatyvios peržiūrėtos ir atnaujintos duomenų apsaugos nuostatos jau dvejetą metų galioja įtvirtinti BDAR, išlieka neaišku, kaip kai kurių BDAR normų taikymas DI atsispindės praktikoje, ar reguliavimas bus tinkamas žmogaus teisėms apsaugoti, ar per daug neapribos inovacijų ir pasieks įstatymų leidėjo tikslą.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai

Tarptautinės sutartys

1. 1948 m. gruodžio 10 d. Visuotinė žmogaus teisių deklaracija, *Valstybės žinios*, 2006-06-17, Nr. 68-2497.
2. 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, iš dalies pakeista protokolais Nr. 11 ir 14, su Pirmuoju Protokolu ir papildomais protokolais Nr. 4, 6, 7, 12, 13 ir 16.
3. 1966 m. gruodžio 19 d. Tarptautinis pilietinių ir politinių teisių paktas, *Valstybės žinios*, 2002-08-02, Nr. 77-3288.
4. 1969 m. lapkričio 22 d. American Convention on Human Rights, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cidh.oas.org/basicos/english/basic3.american%20convention.htm>.
5. 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis, *Valstybės žinios*, 2001-04-13, Nr. 32-1059.
6. 1989 m. lapkricio 20 d. Vaiko teisių konvencija, *Valstybės žinios*, 1995-07-21, Nr. 60-1501.
7. 1990 m. gruodžio 18 d. International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.ohchr.org/EN/ProfessionalInterest/Pages/CMW.aspx>.
8. 1990 m. liepos 1 d. African Charter on the Rights and Welfare of the Child, OAU Doc. CAB/LEG/24.9/49 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.un.org/en/africa/osaa/pdf/au/afr_charter_rights_welfare_child_africa_1990.pdf>.
9. 1990 m. rugpjūčio 5 d. Cairo Declaration on Human Rights in Islam [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.refworld.org/docid/3ae6b3822c.html>.
10. 1994 m. rugsėjo 15 d. Arab Charter on Human rights [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www.humanrights.se/wp-content/uploads/2012/01/Arab-Charter-on-Human-Rights.pdf>.
11. 2009 m. balandžio 24 d. Europos Parlamento rezoliucija dėl Jungtinių Tautų konvencijos dėl žmonių su negalia teisių ir jos fakultatyvinio protokolo pasirašymo

Europos bendrijos vardu [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:184E:0111:0113:LT:PDF>.

12. 2016 m. birželio 7 d. Europos Sąjungos pagrindinių teisių chartija, 2016/C 202/02, OL C 202, 2016 6 7.
13. 2018 m. gegužės 14 d. Nordic Council of Ministers AI in the Nordic-Baltic region [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.regeringen.se/49a602/globalassets/regeringen/dokument/naringsdepartementet/20180514_nmr_deklaration-slutlig-webb.pdf>.

Europos Sąjungos teisės aktai

14. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, OL L 281.
15. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje, OL L 201, 31.7.2002.
16. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR OL L 119, 2016 5 4.
17. 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 (BDAR). OL L 119, 2016.
18. 2018 m. balandžio 10 d. EU Member States Declaration of cooperation on Artificial Intelligence [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/eu-member-states-sign-cooperate-artificial-intelligence>.
19. 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB, PE/31/2018/REV/1, OL L 295, 2018 11 21.

Lietuvos Respublikos įstatymai

20. Lietuvos Respublikos Konstitucija, Lietuvos aidas, 1992-11-10, Nr. 220-0.

21. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas, *TAR*, 2018-07-11, Nr. 11733.
22. Lietuvos Respublikos civilinis kodeksas, *Valstybės žinios*, 2000-09-06, Nr. 74-2262.
23. Lietuvos Respublikos Vyriausybės 2019 m. gegužės 8 d. nutarimas Nr. 461 „Dėl 2019 metų Nacionalinės reformų darbotvarkės patvirtinimo“, *TAR*, 2019-05-14, Nr. 2019-07654.

Užsienio valstybių įstatymai

24. California Consumer Privacy Act of 2018, 1798.100 - 1798.199, Title 1.81.5 added by Stats. 2018, Ch. 55, Sec. 3. [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375&showamends=false>.
25. Constitution de la France, du texte intégral en vigueur, 1958 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.conseil-constitutionnel.fr/le-bloc-de-constitutionnalite/texte-integral-de-la-constitution-du-4-octobre-1958-en-vigueur>.
26. Constitution of Ireland with all amendments, 1937 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.gov.ie/en/publication/d5bd8c-constitution-of-ireland/>.
27. Privacy Act of 1974 5 U.S.C. § 552a As Amended [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cia.gov/library/readingroom/docs/pa.pdf>.
28. U. S. Constitution, the Bill of Rights & All Amendments [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://constitutionus.com>.

Specialioji literatūra

Monografijos

29. YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019.
30. NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018.
31. PETRAITYTĖ, I. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
32. TREPTE, S., et al., *Privacy Online – Perspectives on Privacy and Self-Disclosure in the Social Web*, 2011 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://books.google.lt/books?id=ru2aU0r7sM0C&pg=PA10&lpg=PA10&dq=Westin+1967+AI&source=bl&ots=BLvLjgV-

HI&sig=ACfU3U0dOS38HhprUjzDnPc3VRSAeVNJjA&hl=lt&sa=X&ved=2ahUKEwiLn4Ov2J_oAhVh-SoKHdXXD6gQ6AEwAXoECAkQAQ#v=onepage&q&f=false>.

33. ZALESKIS, J., *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019.

Straipsniai

34. ABHAY, J. S., *et al*. Artificial Intelligence: A Threat to Privacy. *Nirma University Law Journal*, vol. 8, no. 2, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline-org.ezproxy.vdu.lt:2443/HOL/Page?handle=hein.journals/nulj8&id=139&collection=journals&index=>.
35. AJIBADE, O. *A Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330397864_A_Critical_Appraisal_of_Big_Data_Analytics_within_the_General_Data_Protection_Regulation_GDPR_Landscape>.
36. ARNOLD, A. Can Blockchain Help Brands Become GDPR Compliant? 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.forbes.com/sites/andrewarnold/2018/11/20/can-blockchain-help-brands-become-gdpr-compliant/#361b8fdf1203>.
37. BERGGRUEN, N. *et al*. A wakeup call for Europe 2018, *Washington Post*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.washingtonpost.com/news/theworldpost/wp/2018/09/27/europe/>.
38. *Big data, artificial intelligence, machine learning and data protection,* Information Commissioner's Office, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.
39. BOURTOULE, L. *et al*. Machine Unlearning, University of Toronto∗ , Vector Institute§ , University of Wisconsin-Madison, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://arxiv.org/pdf/1912.03817.pdf>.
40. BRKAN, M. Do Algorithms Rule the World? Algorithmic Decision-Making in the Framework of the GDPR and Beyond, *International Journal of Law and Information Technology*, 2019 DOI; 10.1093/ijlit/eay01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901>.

41. BYGRAVE L. A. Minding the Machine v2.0, The EU General Data Protection Regulation and Automated Decision-Making, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019.
42. BYGRAVE, L. A. *Data protection law. Approaching its rationale, logic and limits*. Dordrecht: Kluwer law international, 2002 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/220668128_Data_Protection_Law_Approaching_its_Rationale_Logic_and_Limits_by_L_A_Bygrave>.
43. BYGRAVE, L. A. *Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, Computer Law & Security Review 17(1):17-24, 2001 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/220668128_Data_Protection_Law_Approaching_its_Rationale_Logic_and_Limits_by_L_A_Bygrave>.
44. DE CONCA, S., *et al*. Artificial intelligence and privacy: DI enters the house through the cloud, 2018, iš W. Barfield, & U. Pagallo Eds NUGENT, J., *Research Handbook on the Law of Artificial Intelligence*. Edited by BARFIELD, W., *et al*. Cheltenham, UK; Northampton, USA: Edward Elgar Publishing, 2018.
45. DICK, S. Artificial Intelligence. Harvard Data Science Review, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://hdsr.mitpress.mit.edu/pub/0aytgrau>.
46. GAUBIENĖ, N. *Lietuvos dirbtinio intelekto strategija: ar teisingai suprantamas dirbtinis intelektas?* TeisėPro, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www.teise.pro/index.php/2019/08/26/n-gaubiene-lietuvos-dirbtinio-intelekto-strategija-ar-teisingai-suprantamas-dirbtinis-intelektas/>.
47. GUYNN, J. *Google Photos labeled black people 'gorillas'*, USA today, 2015 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eu.usatoday.com/story/tech/2015/07/01/google-apologizes-after-photos-identify-black-people-as-gorillas/29567465/>.
48. HART, D. M. *When Does Environmental Regulation Stimulate Technological Innovation? Information Technology & Innovation Foundation Report*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://www2.itif.org/2018-environmental-regulation-innovation.pdf>.
49. HILDEBRANDT, M. Data protection by design and technology neutral law, *Computer Law & Security Review* Volume 29, Issue 5, 2013 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://works.bepress.com/mireille_hildebrandt/62/>.

50. HUMERICK, M. Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence, *34 Santa Clara High Tech. L.J.* 393, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/>.
51. JACOBS, S. *et al*. *Data Privacy: Al and the GDPR*, Norton Rose Fulbright, 2017, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.insidetechlaw.com/blog/data-privacy-ai-and-the-gdpr>.
52. JAIN, S. *et al*. Artificial intelligence: threat to privacy. *Nirma University Law Journal*, 8(2), 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/nulj8&div=16&id=&page=>.
53. JEE, C. *Facebook has finally launched its "clear history" button … but it doesn't delete anything*, Silicon Valley, MIT Technology Review, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.technologyreview.com/f/615111/facebook-has-finally-launched-its-clear-history-button-but-it-doesnt-delete-anything/>.
54. KIRBY, M. The history, achievement and future of the 1980 OECD guidelines on privacy, *International Data Privacy Law*, Volume 1, Issue 1, 2010 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://academic.oup.com/idpl/article/1/1/6/759637>.
55. KISS, A. *et al*. Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation iš GUTWIRTH, S. et al. (eds.) *Reforming European Data Protection Law*, Springer, Netherlands [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/312775175_Evolution_or_Revolution_Steps_Forward_to_a_New_Generation_of_Data_Protection_Regulation>.
56. KOKOTT, J. *et al*. The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR, *International Data Privacy Law*, 2013, Vol. 3, No. 4 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/275199054_The_distinction_between_privacy_and_data_protection_in_the_jurisprudence_of_the_CJEU_and_the_ECtHR>.
57. KOOPS, B., *et al*. 'Code' and the Slow Erosion of Privacy, *Michigan Telecommunications and Technology Law Review*, Volume 12, 2005 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr`>.

58. KORFF, D. EC Study on Implementation of Data Protection Directive 95/46/EC [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1287667>.
59. LASKAI, L. *Year in Review: The Year of Data Protection*, Council on Foreign Relations, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cfr.org/blog/year-review-year-data-protection>.
60. LEE, D. *Google executive warns of face ID bias*, BBC, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.bbc.com/news/technology-44977366>.
61. LOHR, J. D., et al. Legal Practitioners' Approach to Regulating AI Risks, iš YEUNG, K., LODGE, M., *Algorithmic Regulation*. Oxford: Oxford University Press, 2019.
62. LYON, H. M. *et al*. *2019 Artificial Intelligence and Automated Systems Annual Legal Review*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.gibsondunn.com/wp-content/uploads/2020/02/2019-artificial-intelligence-and-automated-systems-annual-legal-review.pdf>.
63. MARSH, N. S., Privacy and Human Rights. By James Michael. *International and Comparative Law Quarterly*, British Institute of International and Comparative Law, 1995 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/privacy-and-human-rights-by-james-michael-dartmouth-unesco-publishing-1994-ix-135-text-55-appendices-and-index-pp-isbn-1855213818-5795/BA80F717E512CF28193AB21693582145#>.
64. MAYER-SCHÖNBERGER, V. *et al*. Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation, *Columbia Science & Technology Law Review* Vol. XVII, 2016 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://informationaccountability.org/wp-content/uploads/SchonbergerPadova.pdf>.
65. MC CARTHY, J. *What is Artificial Intelligence?* Computer Science Department Stanford University, 2007 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://perma.cc/U3RT-Q7JK>.
66. MCMANUS, E. *Why did this simple Google Search get retweeted 3,500 times?* Ideas Ted, 2014 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ideas.ted.com/why-did-this-simple-google-search-get-retweeted-3500-times/>.
67. MISHRA, S. *et al*. *Artificial Intelligence Index 2019 annual report*, Stanford Human Centered Artificial Intelligence, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per

internetą: <https://hai.stanford.edu/sites/g/files/sbiybj10986/f/ai_index_2019_report.pdf>.

68. MITROU, L. *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence-Proof'?*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914>.
69. NEAL, B. *A Woman In China Claims That Her iPhone X Was Unlocked By A Coworker's Face, & It's Raising Questions About Diversity In Tech*, Bustle, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/StIiMnE>.
70. NEIDIG, H. *Trump Commerce chief: EU data privacy law could hurt trade*, the Hill, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://thehill.com/policy/technology/389948-wilbur-ross-says-gdpr-could-hurt-trade>.
71. NEMITZ, P. Constitutional Democracy and Technology in the age of Artificial Intelligence, *Royal Society Philosophical Transactions A*, 2018, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3234336>.
72. NORBERG, P. A. *et al*. The privacy paradox: Personal information disclosure intentions versus behaviors, *Journal of Consumer Affairs*, Vol. 41, No.1, 2007, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1745-6606.2006.00070.x>.
73. PARLOFF, R. *Why Deep Learning is Suddenly Changing Your Life*, FORTUNE, 2016, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://fortune.com/longform/ai-artificial-intelligence-deep-machine-learning/>.
74. PEACOCK, S. E. How web tracking changes user agency in the age of Big Data: The used user, *Big data and society*, Vol. 1, No. 2, 2014, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://journals.sagepub.com/doi/10.1177/2053951714564228>.
75. PETRAITYTĖ, I. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.researchgate.net/publication/330722412_Asmens_duomenu_apsaugos_teisinis_reguliavimas_Lietuvos_teises_sistemoje>.
76. POLONSKI, V. *Mitigating algorithmic bias in predictive justice: 4 design principles for AI fairness*, Towards Data Science, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/EtIi5R8>.

77. SATARIANO, A. *et al*. Europe, Overrun by Foreign Tech Giants, Wants to Grow Its Own, *the New York Times*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.nytimes.com/2020/02/19/business/europe-digital-economy.html>.
78. SCHERER, M. U. Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies. *Harvard Journal of Law & Technology*, Volume 29, Number 2, Review, 2016 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://jolt.law.harvard.edu/articles/pdf/v29/29HarvJLTech353.pdf>.
79. SHEPARDSON, D. Trump administration working on consumer data privacy policy iš *Reuters*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.reuters.com/article/us-usa-internet-privacy/trump-administration-working-on-consumer-data-privacy-policy-idUSKBN1KH2MK>.
80. SONI, D. *Understanding the Different Types of Machine Learning Models*, Towards Data Science, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://towardsdatascience.com/understanding-the-different-types-of-machine-learning-models-9c47350bb68a>.
81. TDS, *The Positive and Negative Implications of GDPR* [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr>.
82. United Nations Technology and Innovation report 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://unctad.org/en/PublicationsLibrary/tir2018_en.pdf>.
83. WACHTER, S. et al. Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, *International Data Privacy Law*, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2903469>.
84. WALLACE, N. EU's Right to Explanation: A Harmful Restriction on Artificial Intelligence, TECHZONE360, 2017, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.techzone360.com/topics/techzone/articles/2017/01/25/429101-eus-right-explanation-harmful-restriction-artificial-intelligence.htm>.
85. WARREN, S. D. and BRANDEIS, L. D. The Right to Privacy, *Harvard Law Review*, vol. 4, No. 5, 1890 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <www.jstor.org/stable/1321160>.
86. WESTIN, A. E., Privacy And Freedom, *Washington and Lee Law Review*, Volume 25 Issue 1, 1968 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą:

<https://scholarlycommons.law.wlu.edu/cgi/viewcontent.cgi?article=3659&context=wlulr>.

87. WRIGLEY, S. Bots, Artificial Intelligence and the General Data Protection Regulation: Asking the Right Questions. 22 Trinity C.L. Rev. 199, 2019, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/trinclr22&div=16&id=&page=>.
88. ZARSKY, T. Incompatible: The GDPR in the Age of Big Data, *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3022646>.
89. Zurkus, K. *Understanding California's Consumer Privacy Act: The 'American GDPR'*, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://securityintelligence.com/understanding-californias-consumer-privacy-act-the-american-gdpr/>.

Teismų praktika

90. Europos Sąjungos Teisingumo Teismas. *1980 m. birželio 26 d. sprendimas byloje 136/79 National Panasonic (UK) Limited prieš Europos Bendrijų Komisiją, EU:C:1980:169.*
91. Europos Sąjungos Teisingumo Teismas. *1992 m. balandžio 8 d. sprendimas byloje C-62/90 Komisija prieš Vokietiją, EU:C:1992:169.*
92. Europos Sąjungos Teisingumo Teismas. *2010 m. lapkričio 9 d. sprendimas sujungtose bylose Volker und Markus Schecke GbR (C-92/09) ir Hartmut Eifert (C-93/09) prieš Land Hessen, EU:C:2010:662.*
93. Europos Sąjungos Teisingumo Teismas. *2014 m. gegužės 13 d. sprendimas Google Spain SL ir Google Inc. prieš Agencia Española de Protección de Datos (AEPD) ir Mario Costeja González C-131/12, EU:C:2014:317.*
94. Europos Sąjungos Teisingumo Teismas. *2018 m. birželio 5 d. sprendimas byloje C-210/16 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein prieš Wirtschaftsakademie Schleswig-Holstein GmbH, EU:C:2018:388.*
95. Europos Sąjungos Teisingumo Teismas. *2019 m. rugsėjo 24 d. sprendimas Google LLC prieš Commission nationale de l'informatique et des libertés (CNIL) C-507/17, EU:C:2019:772.*

Soft law* ir *travaux préparatoires

96. 2010 m. lapkričio 23 d. Council of Europe, the Protection of individuals with regard to automatic processing of personal data in the context of profiling, Recommendation CM/Rec(2010)13 and explanatory memorandum [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://rm.coe.int/16807096c3>.
97. 2007 m. birželio 20 d. ES 29 str. Darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf>.
98. 2010 m. vasario 16 d. ES 29 str. darbo grupės Nuomnė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP 169 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.
99. 2013 m. balandžio 3 d. Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.
100. 2014 m. gegužės 5-6 d. International Working Group on Data Protection in Telecommunications, Working Paper on Big Data and Privacy, Privacy principles under pressure in the age of Big Data analytics, 2014 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.edoeb.admin.ch/dam/edoeb/en/dokumente/2014/08/working_paper_onbigdataandprivacyaufenglisch.pdf.download.pdf/working_paper_onbigdataandprivacy.pdf>.
101. 2014 m. rugsėjo 16 d. Article 29 Data Protection Working Party Statement on Statement of the WP29 on the Impact of the Development of Big Data on the Protection of Individuals with Regard to the Processing of Their Personal Data in the EU [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.pdpjournals.com/docs/88352.pdf>.
102. 2015 m. birželio 16 d. Opinion 01/2015 on Privacy and Data Protection Issues relating to the Utilisation of Drones - wp231, 01673/15/EN WP 231 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=640602>.
103. 2017 m. balandžio 5 d. Article 29 Data Protection Working Party, Guidelines on the Right to Data Portability, WP 242 rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga

per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611233>.

104. 2017 m. sausio 10 d. Europos Komisijos Pasiūlymas Europos Parlamento ir Tarybos Reglamentas dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB, COM/2017/010 final - 2017/03 (COD).

105. 2017 m. vasario 16 d. Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl robotikai taikomų civilinės teisės nuostatų (2015/2103(INL)) OL C 252, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A52017IP0051>.

106. 2018 m. balandžio 11 d. Article 29 WP Transparency Guidelines, wp260rev.01, p. 4 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025>.

107. 2018 m. balandžio 25 d. Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Dirbtinis intelektas Europai, COM/2018/237 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/LT/COM-2018-237-F1-LT-MAIN-PART-1.PDF>.

108. 2018 m. gruodžio 7 d. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and The Committee of the Regions Coordinated Plan on Artificial Intelligence, COM/2018/795 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence>.

109. 2018 m. kovo 9 d. European Group on Ethics in Science and New Technologies, *Statement on Artificial Intelligence, Robotics and 'Autonomous' Systems* [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://ec.europa.eu/research/ege/pdf/ege_ai_statement_2018.pdf>.

110. 2018 m. spalio 15 d. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108) Report on Artificial Intelligence, *Artificial Intelligence and Data Protection: Challenges and Possible Remedies*, T-PD(2018)09Rev [interaktyvus. Žiūrėta 2020-03-17]. Prieiga

per internetą: <https://rm.coe.int/report-on-artificial-intelligence-artificial-intelligence-and-data-pro/16808e6012>.

111. 2018 m. vasario 6 d. Article 29 Data Protection Working Party Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP251rev.01 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053>.

112. 2019 m. balandžio 8 d. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Building Trust in Human Centric Artificial Intelligence, COM(2019) 168 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence>.

113. 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Policy and investment recommendations for trustworthy Artificial Intelligence [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>.

114. 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Definition of AI: Main Capabilities and Disciplines [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/definition-artificial-intelligence-main-capabilities-and-scientific-disciplines>.

115. 2019 m. balandžio 8 d. High-Level Expert Group on Artificial Intelligence Policy and investment recommendations for trustworthy Artificial Intelligence, [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/digital-single-market/en/news/policy-and-investment-recommendations-trustworthy-artificial-intelligence>.

116. 2019 m. lapkričio 12 d. European Data Protection Board Guidelines 3/2018 on the territorial scope of the GDPR [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en.pdf>.

117. 2020 m. vasario 19 d. White Paper on Artificial Intelligence - A European approach to excellence and trust, COM/2020/65 final [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_lt.pdf>.

Kiti šaltiniai

118. 2019 m. kovo 8 d. Lietuvos Dirbtinio intelekto strategija [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <http://kurklt.lt/wp-content/uploads/2019/04/DI_strategija_LT_koreguota.pdf>.

119. *Artifical intelligence and privacy*, Norvegian Data Protection Authority, Datatilsynet, 2018 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf>.

120. *Comment permettre à l'homme de garder la main?*, Commission nationale informatique et libertes, 2017 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf>.

121. European Union Agency for Fundamental Rights Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf>.

122. KUZIEMSKI, M. *et al*. AI Governance Post-GDPR: Lessons Learned and the Road Ahead, European University Institute, Policy brief, 2019 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cadmus.eui.eu/bitstream/handle/1814/64146/STG_PB_2019_07-EN.pdf?sequence=1&isAllowed=y>.

123. National Conference of State Legislatures *2019 Consumer Data Privacy Legislation*, 2020 [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx>.

124. Organisation for Economic Cooperation and Development. *AI policies and initiatives, Overview of AI national policy responses*, OECD Library [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://cutt.ly/AtIiS72>.

125. VON DER LEYEN, U. *My agenda for Europe. Political Guidelines for the Next European Commission 2019-2024* [interaktyvus. Žiūrėta 2020-03-17]. Prieiga per internetą: <https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf>.

SANTRAUKA

ES Bendrojo duomenų apsaugos reglamento taikymo dirbtiniam intelektui ypatumai

Sparčiai besivystant ir plačiai pritaikant dirbtinio intelekto (DI) technologiją renkami ir naudojami neaprėpiami kiekiai asmens duomenų, kas neužtikrinant atitinkamų saugiklių ir priežiūros globaliu mastu kelia iššūkius asmenų teisėms į privatumą ir duomenų apsaugą. Turint omenyje, jog 90 % viso pasaulio duomenų buvo sukurti per pastaruosius penkerius metus, atitinkamas prisitaikymas reikalingas ir iš duomenų apsaugos reguliavimo perspektyvos. Ypatingas žingsnis duomenų apsaugos srityje žengtas priėmus Bendrąjį duomenų apsaugos reglamentą (BDAR). Sugriežtintos duomenų privatumo taisyklės ne tik pradėjo naują duomenų apsaugos reguliavimo etapą ES, bet kartu tapo pavyzdžiu bei atspirties tašku ir kitiems įstatymų leidėjams bei technologijų vystytojams visame pasaulyje.

DI kontekste daugiausia reikšmės BDAR reguliavime įgyja pritaikytosios ir standartizuotosios duomenų apsaugos bei automatizuoto atskirų sprendimų priėmimo, įskaitant profiliavimą, kategorijos. Taip pat reikšmingą įtaką DI asmens duomenų tvarkymo veiklai daro teisėtumo, sąžiningumo ir skaidrumo, duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo principai bei duomenų subjektams užtikrinta teisė būti pamirštam ir teisė į duomenų perkeliamumą.

Pirmoje darbo dalyje nagrinėjama DI apibrėžties problematika, privatumo ir duomenų apsaugos koncepcijų skirtis, atskleidžiamas DI reguliavimo poreikis, įvertinama reguliavimo pažanga ir priemonės ES, Lietuvoje ir JAV. Antroje darbo dalyje dėmesys sutelkiamas į BDAR kaip DI reguliavimo šaltinį, aptariami esminiai reguliavimo bruožai ir reguliavimo taikymo DI prielaidos. Trečioje darbo dalyje vertinamas BDAR numatytų duomenų apsaugos principų poveikis DI, tuomet analizuojama konkrečių BDAR numatytų duomenų subjektų teisių ir iš jų kylančias pareigų DI pasitelkiančiam subjektui poveikis. Darbe apsiribojama tik didžiausią problematiką DI reguliavimui keliančių BDAR aspektų analize.

SUMMARY

Peculiarities of Application of the EU General Data Protection Regulation for Artificial Intelligence

Rapid development and widespread application of artificial intelligence (AI) technology lead to the collection and use of an infinite amount of personal data, which, without adequate safeguards and supervision, at a global level poses a challenge to individuals' rights to privacy and data protection. Given that 90% of global data have been created over the last five years, appropriate adaptation is inevitably necessary from a data protection regulatory perspective. A particular step in the area of data protection has been taken by the adoption of the General Data Protection Regulation (GDPR). Tightened data privacy rules have not only begun a new phase of data protection regulation in the EU but have also become an example and a starting point for other legislators and technology developers around the world.

In the context of AI, data protection by design and by default and automated individual decision-making, including profiling, clauses are of major importance in GDPR regulation. Nevertheless, the principles of lawfulness, fairness and transparency, purpose limitation, data minimization and data subjects‘ right to be forgotten and the right to data portability also have a significant impact on the AI processing of personal data.

The first part of the thesis addresses the issues of definition of AI, differences in privacy and data protection concepts, reveals the need for AI regulation, assesses regulatory progress and measures in the EU, Lithuania and the US. The second part of the work focuses on GDPR as a source of AI regulation, discusses key regulatory features and preconditions for the application of regulation to AI. The third part of the thesis assesses the impact of the application of GDPR principles on AI, followed by the study of specific rights of the data subject and the obligations arising therefrom for an entity using AI. The work is limited to the analysis of the most problematic aspects of GDPR for the regulation of AI.