Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Augustės Abukauskaitės
V kurso, tarptautinės ir Europos Sąjungos teisės
studijų šakos studentės

Magistro darbas

Didžiųjų duomenų (*big data*) reguliavimas pagal ES Bendrąjį duomenų apsaugos reglamentą
Regulation of Big Data under the EU General Data Protection Regulation

Vadovas: asist. dr. Julius Zaleskis

Recenzentas: doc. dr. Lauras Butkevičius

Vilnius
2021

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame magistro darbe yra analizuojamas ES Bendrasis duomenų apsaugos reglamentas, jo nuostatų taikymo praktika didiesiems duomenims ir jų analizei. Taip pat šiame darbe atskleidžiami ryškiausi ES Bendrojo duomenų apsaugos reglamento nuostatų taikymo didiesiems duomenims ir jų analizei probleminiai aspektai.

Pagrindiniai žodžiai: didieji duomenys, didžiųjų duomenų analizė, privatumas, duomenų apsaugos teisė, BDAR.

The master's thesis examines the application of the EU General Data Protection Regulation provisions to Big Data practice. This paper also reveals the main problematic aspects of applying the EU General Data Protection Regulation provisions within the context of big data and its analysis.

Keywords: big data, big data analysis, privacy, data protection law, GDPR.

TURINYS

ĮVADAS

Darbo temos aktualumas. Didieji duomenys, daiktų internetas, dirbtinis intelektas, „Blockchain" ir kitos novatoriškos technologijos pastaraisiais metais tapo dominuojančiomis informacinių technologijų tendencijomis (Forgó *et al*., 2017, p. 17). Didžiųjų duomenų, kaip ir kitų informacinių technologijų, suvokimas teisiniame kontekste iš esmės skiriasi nuo kitų dalykų, reguliuojamų bendrosios teisės sistemos, kuri kūrybiškai ir nuspėjamai vystosi virš savo pradinių tikslų (Holmes, 1881, cituota Devins *et al*., 2017, p. 360). Didžiųjų duomenų atsiradimas ir plėtra laikomi vienais didžiausių iššūkių, su kuriais susiduria duomenų apsaugos įstatymai (Zarsky, 2017, p. 996). Pastaraisiais metais Europos Sąjungoje kilo nemažai diskusijų, susijusių su duomenų analize ir valdymu, keliant klausimus: ar vartotojai vis dar gali kontroliuoti savo skaitmeninę tapatybę? (Colangelo, Maggiolino, 2018, p. 224); ar įmanoma užtikrinti automatizuotų sprendimų sąžiningumą ir nešališkumą?; ar apskritai yra įmanoma suderinti didžiųjų duomenų veikimą su asmenų teisėmis ir laisvėmis, tuo pačiu metu užtikrinant duomenų apsaugą ir neapsunkinant didžiųjų duomenų organizacijų veiklos? Įtampa kyla tarp nuolatinio noro apsaugoti asmens duomenis taikant naują, technologiniu neutralumu pasižymintį ir tvirtą teisinį režimą – Europos Sąjungos reglamentą dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau – BDAR), dėl kurio kai kurios duomenų analizės rinkimo formos tampa neteisėtos, ir tarp tikslo generuoti ir išanalizuoti kuo daugiau (asmens) duomenų, kad Europa galėtų išlikti konkurencinga pasauliniame „duomenų mūšyje" (Delcker, 2020, cituota Finck, Biega, 2021, p. 2). Taigi vienu metu vyrauja politinės paskatos tvarkyti tiek mažiau, tiek daugiau duomenų (Finck, Biega, 2021, p. 2). Ši įtampa akivaizdžiai įžvelgiama diskusijose dėl duomenų apsaugos teisės principų taikymo didžiųjų duomenų reguliavimui. Be to, didėjantis duomenų kiekis ir apdorojimo galimybės, apimančios algoritminį profiliavimą, personalizavimą ir sprendimų priėmimo sistemas kelia vis daugiau iššūkių siekiant užtikrinti įstatymų atitiktį, apsaugoti asmenis bei atrasti naujų techninių galimybių siekiant sąžiningo ir teisėto technologijų panaudojimo (Finck, Biega, 2021, p. 2). Didžiųjų duomenų analitinis apdorojimas turi didžiulį potencialą, tačiau taip pat kelia didelius iššūkius, kuriuos nagrinėja, aiškina bei sprendžia teisininkų ir technologijų specialistų bendruomenė.

Darbo tikslas. Magistro darbo tikslas yra išanalizuoti pagrindines BDAR nuostatas, jų taikymą didžiųjų duomenų reguliavimui bei šių nuostatų ir didžiųjų duomenų tarpusavio santykio problematiką.

Darbo uždaviniai. Magistro darbo tikslui pasiekti yra keliami šie uždaviniai:

1. Atskleisti didžiųjų duomenų ir duomenų apsaugos teisės sąveiką;
2. Identifikuoti pagrindinius duomenų apsaugos teisės šaltinius, taikomus didžiųjų duomenų reguliavimui;
3. Išnagrinėti pagrindines BDAR nuostatas didžiųjų duomenų ir jų analizės kontekste;
4. Išanalizuoti BDAR taikymo didiesiems duomenims pagrindines problemas.

Darbo objektas. Šio darbo objektą lemia analizuojamai temai atskleisti nustatytas tikslas ir išsikelti uždaviniai. Darbo objektą sudaro BDAR nuostatos, jų taikymo praktika didiesiems duomenims. Pagrindinis dėmesys skiriamas principams, kurie kelia didžiausią problematiką didžiųjų duomenų ir jų analizės kontekste. Darbe nagrinėjami duomenų kiekio mažinimo ir tikslo apribojimo principai, kurie neretai laikomi ribojantys didžiųjų duomenų pranašumus bei tikslumo principas, kurio svarba akivaizdi didžiųjų duomenų analizės sprendimų priėmimo metu. Magistro darbe, tačiau ne atskiruose skyriuose, taip pat remiamasi saugojimo trukmės apribojimo, pritaikytosios ir standartizuotosios duomenų apsaugos principais. Šiems principams neskirtos atskiros dalys, tačiau jų sąsaja minima nagrinėjant kitas BDAR nuostatas. Be to, analizuojami tik didžiausius iššūkius, teorinius ir praktinius neaiškumus didžiųjų duomenų kontekste keliantys kiti BDAR reikalavimai, įskaitant teisę susipažinti su tvarkomais duomenimis, teisę į duomenų pekeliamumą, teisę būti pamirštam, automatizuotą sprendimų priėmimą. Taip pat analizuojamas ir poveikio duomenų apsaugai vertinimas, kuris neretai kelia neaiškumus dėl jo poreikio ir galimų įgyvendinimo metodų.

Tyrimo metodai. Magistro darbe yra naudojami šie tyrimo metodai:

1. Lingvistinis – Pirmiausia, šis metodas naudojamas siekiant išanalizuoti didžiųjų duomenų ir jų analizės sampratą. Taip pat metodas naudojamas siekiant atskleisti pagrindinių BDAR nuostatų reikšmę, jų turinį, pagrindines taikymo sąlygas bei išimtis.
2. Istorinis – Šis metodas naudojamas analizuojant didžiųjų duomenų suvokimo raidą. Taip pat metodas naudojamas identifikuojant pagrindinius duomenų apsaugos teisės šaltinius, taikomus didžiųjų duomenų reguliavimui, kadangi atsižvelgiama ir į šaltinių pokyčius laiko ir technologijų pažangos kontekste.

3. Lyginamasis – Šis metodas naudojamas lyginant BDAR ir 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau - Duomenų apsaugos direktyva) nuostatas.
4. Sisteminis – Metodas naudojamas sistemiškai aiškinant BDAR nuostatas.
5. Teleologinis – Darbe atsižvelgiama ir į filosofinį aiškinimą, pritaikant filosofines metaforas, kad būtų atskleistas didžiųjų duomenų analizės technologijų ir teisės nuostatų tarpusavio ryšio suvokimas.
6. Loginis – Šis metodas dažniausiai naudojamas probleminių aspektų apibendrinime bei išvadose.

Darbo originalumas. Užsienio autorių, rašiusių didžiųjų duomenų tema, yra nemažai, tačiau daugumoje iš autorių straipsnių ir monografijų analizuojamos tik atskiros, didiesiems duomenims taikomos, nuostatos. BDAR nuostatų taikymo didiesiems duomenims problematika dėl specialiųjų duomenų kategorijų, automatizuoto sprendimų priėmimo, duomenų tikslumo ir duomenų kiekio mažinimo principų išsamiai nagrinėta autoriaus Tal. Z. Zarsky straipsnyje ,,Incompatible: The GDPR in the age of Big Data". Taip pat moksliniame straipsnyje ,,Reviving purpose limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems" autorės Asia Biega and Michèle Finck detaliai aptarė pagrindines diskusijas keliančių duomenų apsaugos teisės principų taikymą didžiųjų duomenų technologijoms. Be to, BDAR nuostatų taikymas didiesiems duomenims bendrinių aspektų prasme atskleidžiamas autorių P. Voigt ir A. Von dem Bussche praktiniame gide ,,The EU General Data Protection Regulation (GDPR). Pagrindinę didžiųjų duomenų analizės veiklą – automatizuotą sprendimų priėmimą plačiai analizavo autoriai S. Wachter, B. Mittelstadt, C.Russell moksliniame straipsnyje ,,Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI".

Didžiųjų duomenų tema Viliaus universiteto Teisės fakultete yra parašytas R. Lipeikaitės magistro darbas ,,Didieji duomenys, duomenų apsauga ir piktnaudžiavimas dominuojančia padėtimi: konkurencijos teisės normų aiškinimo ir taikymo problemos Europos Sąjungoje ir JAV". Tačiau, šis magistro darbas atspindi didžiųjų duomenų taikymą iš konkurencijos teisės perspektyvos. Taip pat panašia tema Vilniaus universiteto Teisės fakultete yra parašytas K. Seliutaitės magistro darbas ,,ES Bendrojo duomenų apsaugos reglamento taikymo dirbtiniam intelektui ypatumai". Didžiųjų duomenų tema yra susijusi su dirbtiniu intelektu, kuomet

atliekama didžiųjų duomenų analizė, todėl magistro darbe, kuomet reikalavimai yra susiję su didžiųjų duomenų analize, aptariami kai kurie tie patys BDAR principai ir kiti reikalavimai. Tačiau, šiems aspektams analizuoti dažniausiai naudojami skirtingi šaltiniai, pateikiami skirtingi praktiniai pavyzdžiai bei išskiriami kiti probleminiai aspektai.

Magistro darbas iš kitų magistro darbų ir mokslinių straipsnių išsiskiria bendra užsienio literatūros ir lietuvos autorių didžiųjų duomenų ir bendrųjų duomenų apsaugos teisės šaltinių analize ir susisteminimu.

Svarbiausi šaltiniai. Visų pirma, pagrindinis magistro darbo šaltinis yra BDAR. Taip pat viso darbo metu remiamasi J. Zaleskio monografija ,,Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“, kurioje pateikta išaiškinimų visų BDAR nuostatų klausimais. Be to, aiškinant BDAR viso darbo metu taip pat yra remiamasi ES 29 str. Darbo grupės nuomonėmis. Taip pat magistro darbe plačiai naudojami JK Informacijos komisaro tarnybos *soft law* šaltiniai, atskleidžiantys pagrindinių BDAR ir JK duomenų apsaugos teisės akto nuostatų taikymą didžiųjų duomenų praktikoje. Be to, bendriniam nuostatų suvokimui ir atskleidimui plačiai naudojamas autorių P. Voigt ir A. Von dem Bussche praktinis gidas ,,The EU General Data Protection Regulation (GDPR).

BDAR taikymo didiesiems duomenims ir (ar) jų problematikos klausimais dažniausiai remiamasi S. Wachter, A. Selbst, J. Powles, B. Goodman, S. Flaxman, C. Kuner, T. Z. Zarsky, B. Mittelstadt, C. Russell, M.E Kaminski, G. Malgieri ir kitų žymių duomenų apsaugos, privatumo ar informacinių technologijų teisės autorių moksliniais straipsniais. Principų analizėje dažniausiai naudojamas autorių Asia Biega and Michèle Finck straipsnis ,,Reviving purpose limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems”. Automatizuoto sprendimų priėmimo ir diskriminacijos problematikos atžvilgiu išsamiai remiamasi autorių S. Wachter, B. Mittelstadt, C.Russell moksliniu straipsniu ,,Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI”. Be to, šiai problematikai analizuoti naudojamas M. Rhoen ir QY Feng straipsnis ,, Why the ‘Computer says no’: illustrating big data’s discrimination risk through complex systems science”. Duomenų perkeliamumo teisei atskleisti daugiausia remiamasi P. De Hert., V. Papakonstantinou, G. Malgieri., L. Beslay ir I.Sanchez straipsniu ,,The right to data portability in the GDPR: Towards user-centric interoperability of digital services”. Šių išvadintų teisių ir kitų teisių analizei taip pat taikomi ir kiti rečiau darbe minimi moksliniai šaltiniai.

1. DIDIEJI DUOMENYS IR DUOMENŲ APSAUGOS TEISĖ

1.1. Didieji duomenys kaip technologija: samprata ir charakteristikos

Didieji duomenys (angl. *big data*) paprastai suprantami kaip dideli, įvairios informacijos rinkiniai, kurie auga vis didesniu greičiu (Gandomi, Haider, 2015, p. 137). Vieningo ir tikslaus didžiųjų duomenų apibrėžimo nėra net ir šiomis dienomis. Pradžioje didžiųjų duomenų terminas reiškė duomenų rinkinius, kurių apimtis tapo problema juos tvarkant (Organisation for Economic Co-operation and Development, 2013, p. 11). Panašus suvokimas pasižymi ir daugelyje šių dienų apibrėžimų. Autorius M. Loukides didžiuosius duomenis įvardino kaip duomenis, kurių „problemos dalis tampa pats duomenų dydis“. Pasaulinis institutas „McKinsey” didžiuosius duomenis apibūdino kaip duomenis, kurių „dydis viršija tipinių duomenų bazių programinės įrangos įrankių galimybes užfiksuoti, saugoti, valdyti ir analizuoti“ (Organisation for Economic Co-operation and Development, 2013, p. 11). Didžiųjų duomenų apibrėžtys skirtingų autorių darbuose paprastai yra panašios, tačiau vyraujant dideliam „*big data*” kintamumui ir besiplečiančiai technologinei įvairovei pasiekti vieningą apibrėžimą sunkiai įsivaizduojama.

Didiesiems duomenims būdingos specialios charakteristikos. Autorius Douglas B. Laney 2001 m. pabrėžė tris pagrindines didžiųjų duomenų charakteristikas – apimtį, įvairovę ir spartą (angl. – *volume, variety, velocity*) (Diebold, 2012, cituota Patgiri, 2016, p. 18). Charakteristikos pasirodė daug vėliau nei pirmą kartą buvo paminėtas didžiųjų duomenų terminas (Gandomi, Haider, 2015, p. 138), tačiau atnešė svarbų indėlį didžiųjų duomenų identifikacijai. Šiomis dienomis priskiriama ir daugiau didžiųjų duomenų savybių, kaip teisingumas, vertė (angl. – *veracity, value*) ir kt. (Patgiri, 2016, p. 18). Bendrąja prasme charakteristikos yra:

1. Apimtis (angl. *volume*) – Duomenų apimtis gali pasiekti precedento neturintį lygį. Didieji duomenys apima nuo eksabaitų iki zetabaitų, ateityje akivaizdu pasiekti dar neapibrėžtus duomenų dydžius. Technologija turi užtikrinti, kad būtų galima susidoroti su didėjančiu duomenų kiekiu (Patgiri, 2016, p. 19).
2. Sparta (angl. *velocity*) - Duomenų dydis auga eksponentiškai, ir taip prisideda prie didesnės duomenų bazės (Laney, 2001, cituota Patgiri, 2016, p. 19). Sparta apima keletą skirtingų faktorių. Pirmiausia, lemiamą poveikį turi interneto vartotojų augimas.

Interneto naudotojų daugėja kas dieną, o kiekvienas iš jų tame tarpe pateikia, ar besinaudodamas internetu leidžia sukurti vis daugiau duomenų (Patgiri, 2016, p. 19). Be to, daiktų interneto (angl. *internet of things)* atsiradimas yra vienas svarbiausių didžiųjų duomenų augimo indėlių. Pavyzdžiui, jutiklių įtaisai, stebėjimo kameros yra žinomi didžiųjų duomenų generatoriai (Patgiri, 2016, p. 20). Taip pat didžiųjų duomenų spartą lemia ir debesų kompiuterija, kuriai vystantis gaunami didžiuliai duomenys, reikalaujantys atsakingo saugojimo, valdymo ir apdorojimo (Patgiri, 2016, p. 20).

3. Įvairovė (angl. *variety*) - Didžiuosius duomenis sudaro struktūrizuoti, nestruktūruoti ir pusiau struktūrizuoti duomenys (Patgiri, 2016, p. 20). Struktūrizuoti duomenys yra gaunami iš tradicinių duomenų bazių sistemų arba gali būti prie jų pridėti. Nestruktūrizuoti ar pusiau struktūrizuoti duomenys gaunami iš tinklalapių, paieškos indeksų, socialinės žiniasklaidos forumų, el. pašto ir kitų sistemų. Pavyzdžiui, „Facebook , „Twitter" ar kt. (Aggarwal *et al.*, 2015, p. 50).
4. Teisingumas (angl. – *veracity*) – Teisingumo charakteristika savotiškai reiškia tikslumą ir prasmingumą (Xiaolong *et al.*, 2015, cituota Patgiri, 2016, p. 20). Netikslūs duomenys gali sukelti neteisingą nurodymą ar sprendimą. Pavyzdžiui, rekomenduojant vartotojams kurį nors produktą, netikslūs rezultatai galėtų sumažinti galimas pajamas (Patgiri, 2016, p. 20).
5. Vertė (angl. – *value*) – Didžiųjų duomenų vertė nėra vien tik duomenų rinkimas, bet ir iš jų gautos įžvalgos. Vertė sukuriama apdorojant didžiųjų duomenų rinkinius (Custers, Uršic, 2016, p. 4).
6. Kintamumas, netinkamumas, pastovumas ir k.t. (Patgiri, 2016, p. 21).

Vertės charakteristika pasižymi iš didžiųjų duomenų gaunant tam tikras įžvalgas (Custers, Uršic, 2016, p. 4). Didžiųjų duomenų terminas apima ne tik pačius duomenis, bet ir jų analizę (angl. *big data analysis*) (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 350). Dirbtinio intelekto (angl. *artificial intelligence*) ir mašininio mokymosi (angl. *machine learning*) technologijų pagalba duomenys yra apdorojami ir išgaunami atitinkami rezultatai. Didžiausios interneto kompanijos, tokios kaip „Google", „Facebook", „Amazon", vienoje ar kitoje formoje užsiima didžiaisiais duomenimis, o duomenis laiko pagrindiniu vertės kūrimo turtu ir šaltiniu (Rubinstein, 2013, p. 76). Pavyzdžiui, „Google" moko savo paieškos algoritmus bei kuria naujas ir daug duomenų reikalaujančias paslaugas,

tokias kaip balso atpažinimas, vertimas ir vietos nustatymas (Markoff, 2012, cituota Rubinstein, 2013, p. 76). Didžiųjų duomenų analizė teikia naudą ne tik minėtiems interneto milžinams, bet ir kitoms stambioms įmonėms ar vyriausybės agentūroms, kurios remiantis statistiniais metodais ir duomenų gavybos algoritmais įgauna galimybę pagerinti sprendimų priėmimo procesus (Rubinstein, 2013, p. 76). Didžiųjų duomenų analizė lemia teigiamus rezultatus įvairiose srityse. Pasaulinio instituto „McKinsey“ ataskaitos rodo teigiamą poveikį įvairiuose sektoriuose, pavyzdžiui, tokiuose kaip sveikatos apsauga ar mažmeninė prekyba (Manyika *et al.*, 2011, cituota Tene, Polonetsky, 2012, p. 244). Paprastai tariant, didieji duomenys yra laikomi turtu, kurį sunku išnaudoti. Dirbtinis intelektas gali būti vertinamas kaip raktas siekiant atrinkti didžiųjų duomenų vertę, o mašininis mokymasis yra vienas iš techninių mechanizmų, kuris palaiko ir palengvina dirbtinį intelektą. Visų trijų sąvokų derinį galima pavadinti „didžiųjų duomenų analitika“ (angl. *big data analytics*) (Information Commissioner‘s Office, 2017, p. 8).

Taigi didieji duomenys vieningo apibrėžimo neturi, tačiau, manoma, kad juos naudinga laikyti duomenimis, kuriuos dėl kelių skirtingų charakteristikų sunku analizuoti naudojant tradicinius metodus (Information Commissioner‘s Office, 2017, p. 6). Didieji duomenys apima ne tik pačius duomenis, bet ir jų analizę, kurios metu gautos įžvalgos susilaukia teigiamų ir pažangių rezultatų tiek viešajame, tiek privačiame sektoriuje (Information Commissioner‘s Office, 2017, p. 3).

1.2. Asmens duomenų apimtis didžiųjų duomenų kontekste

Didieji duomenys (angl. *big data*) sudaro tiek asmens, tiek ne asmens duomenis, ką patvirtina viena iš pagrindinių didžiųjų duomenų charakteristikų – įvairovė (angl. – *variety*). Ne asmens duomenys gali sudaryti informaciją apie klimatą, palydovinius vaizdus (Jourová, 2016, p. 1), GPS duomenis, galinčius nustatyti transporto priemonių atvykimo laiką, duomenis iš radijo teleskopų, laivuose gabenamų konteinerių jutiklių ir kitus įvairius duomenis ir jų analizės metodus, kuriuose duomenų analizė leidžia naudoti naujus atradimus ir pagerinti paslaugas bei verslo procesus nenaudojant asmens duomenų (Information Commissioner‘s Office, 2014, p. 11). Didieji duomenys gali apimti ir asmens duomenis. Didžiųjų duomenų visuma gali būti susijusi su asmens duomenimis arba yra pačių technologijų veikimo pagrindas. Didieji duomenys gali apimti visą su asmeniu susijusią informaciją, ir tai gali būti vardas, pavardė,

telefono numeris, nuotrauka, elektroninio pašto adresas, banko duomenys, įrašai socialinės tinklaveiklos svetainėse, medicininė informacija ar kompiuterio IP adresas (Jourová, 2016, p. 1). Be to, didieji duomenys sudaro galimybes vadovaujantis didžiųjų duomenų analize sukurti naujus asmens duomenis. Paprastai tariant, duomenis, kurių asmuo pats nepateikė, bet kurie buvo sugeneruoti analizės būdu. Pavyzdžiui, socialinė žiniasklaida gali padėti išanalizuoti asmens gyvenimo būdą kaip veiksnį nustatantį jo kredito reitingą ar asmeniui gresiančią sveikatos būklę (Information Commissioner‘s Office, 2014, p. 11).

Autoriai teigia, jog didžiųjų duomenų analizės kontekste ši asmens ir ne asmens duomenų atskirtis gali tapti sudėtinga. Atskirties iššūkiai taip pat reikalauja analizės ir tam skirtų metodų. Atskirties problemos gali pasireikšti analizuojant didžiųjų duomenų rinkinius, o skiriamosios linijos tarp asmens duomenų ir ne asmens duomenų nubrėžimas daro lemiamą įtaką siekiant nustatyti duomenų apsaugos įstatymų taikymo sritį (Finck, Pallas, 2020, p. 11).

1.3. Didžiųjų duomenų ir duomenų apsaugos teisės sąveika

1.3.1. Didieji duomenys, privatumas ir duomenų apsauga

Asmenis, kuriems kyla grėsmė tvarkant jų asmens duomenis, saugo teisė į privatumą. Žodis „privatumas” įvardija asmens teisės objektą, t.y. gėrį, kurį saugo teisė. Teisė į privatumą (arba privataus gyvenimo apsauga) reiškia asmens subjektyvią teisę tą gėrį apsaugoti ir šios teisės turinį (Meškauskienė, 2015 cituota Zaleskis, 2019, p. 38).

Duomenys žada didelę ekonominę ir socialinę naudą, tačiau taip pat kelia rimtą susirūpinimą dėl privatumo (Rubinstein, 2013, p. 74). Paprastai tariant, didžiųjų duomenų, apimančių asmens duomenis, analizavimas, saugojimas, apdorojimas ar bet koks kitas tokių duomenų tvarkymas kelia grėsmę asmenims bei jų privatumui. Didieji duomenys kelia iššūkių privatumui, todėl yra saugomi teisės į privatumą apimtimi (Altman *et al*., 2018, p. 31). Didieji duomenys nuolatos naudojami atliekant išilginius tyrimus, todėl juos sudaro daugybė su asmenimis susijusių savybių. Privatumo įstatymų, politikos ir praktikos vykdymas šiose salygose yra būtinybė apsaugoti asmenis ir grupes nuo informacinės žalos, susijusios su informacijos apie juos vertinimu ir dalijmusi (Altman *et al*., 2018, p. 31).

Privataus gyvenimo apsauga yra neatsiejama nuo duomenų apsaugos. Teisė į privatų gyvenimą ir teisė į duomenų apsaugą, nors ir glaudžiai susijusios, yra skirtingos teisės

(Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 21). Glaudi šių teisių sąsaja pasižymi persidengiančia paskirtimi. Tarptautinėje doktrinoje privatumas apibrėžiamas keturiomis grupėmis (Bygrave, 2020, cituota Zaleskis, 2019, p. 38). Pirmojoje grupėje privatumas apibrėžiamas per nesikišimą į asmens gyvenimą. Antroji grupė yra glaudžiai susijusi su pirmąja ir privatumą apibrėžia per prieigos prie asmens ribojimą (Zaleskis, 2019, p. 38). Trečiojoje grupėje privatumas suprantamas kaip asmenų atliekama informacijos apie juos kontrolė. Toks požiūris į privatumą iš esmės tapatinamas su duomenų apsauga (Zaleskis, 2019, p. 39). Ketvirtosios grupės apibrėžimai susiaurina privatumą iki intymių ir jautrių asmens gyvenimo aspektų apsaugos (Zaleskis, 2019, p. 39). Duomenų apsauga yra vienas iš privataus gyvenimo elementų. Persidengianti paskirtis pasižymi tuo, kad privatumas yra vienas iš duomenų apsaugos teisės tikslų. Duomenų apsaugos teisės saugomas privatumas yra pagrindinė žmogaus teisė ir konstitucinė vertybė pagarba asmeniui grįstoje visuomenėje (Zaleskis, 2019, p. 39).

Didieji duomenys kelia susirūpinimą dėl asmenų privatumo, tuo tarpu privatumas yra vienas iš duomenų apsaugos teisės tikslų, tad didieji duomenys ir jų analizė negalėtų veikti be duomenų apsaugos ir jos nustatyto reguliavimo. Reguliavimas pasižymi didele svarba įgyvendinant asmens duomenų tvarkymą ir panaudojimą didžiųjų duomenų kontekste, tačiau pereinant prie reguliavimo svarbu atskleisti duomenų apsaugos teisės sampratą.

Duomenų apsaugos teisę apibrėžti nėra paprasta, taip pat visuotinai pripažįstamo apibrėžimo teisės aktuose ieškoti nereikėtų, tačiau pasiūlyti tokį apibrėžimą yra teisės doktrinos ir kitų antrinių teisės šaltinių funkcija (Zaleskis, 2019, p. 29). Autoriai ir teisės mokslininkai yra suformulavę nemažai apibrėžimų, įvardijančių duomenų apsaugos teisės reikšmę ir pagrindines funkcijas. Šiuolaikinė teisės doktrina duomenų apsaugą apibrėžia kaip priemonių (teisinių ir/ ar neteisinių), skirtų apsaugoti asmenis nuo žalos, kurią sukelia informacijos apie juos tvarkymas (automatiniu ir/ ar rankiniu būdu) ir apimančių tam tikrus principus, išdėstytus pripažįstamuose dokumentuose, rinkinį (Bygrave, 2002, cituota Zaleskis, 2019, p. 30). Apibrėžimas ir didžiųjų duomenų charakteristikos akivaizdžiai nusako, jog didieji duomenys renkami automatiniu būdu, automatinėmis priemonėmis vyksta jų apdorojimas bei dažniausiai automatiniu būdu atliekama jų analizė.

1.3.2. Didžiųjų duomenų reguliavimas asmens duomenų apsaugos teisėje

1.3.2.1. Reguliavimas tarptautinėje teisėje

Asmens duomenys, sudarantys didžiųjų duomenų rinkinius, pirmiausia yra reguliuojami bendraisiais duomenų apsaugos teisės šaltiniais. Jungtinės Tautos nepripažįsta asmens duomenų apsaugos kaip pagrindinės teisės, tačiau teisė į privatumą jau seniai įtvirtinta tarptautiniu lygmeniu (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 21). Autoriai Samuel D. Warren ir Louis D. Brandeis pirmieji iškėlė mintį, kad privatumas yra vertas teisinės apsaugos (Brandeis, Warren, 1890, cituota Krishnamurthy, 2020, p. 26). Teisė į privatumą yra išskirtinė tarp pagrindinių pilietinių ir politinių teisių, kadangi tarptautinėje teisėje ji buvo įtvirtinta tuo metu, kai jos visapusiškai negarantavo nė vienos iš valstybių konstitucinė sistema (Digglemann, Cleis, 2014, cituota Krishnamurthy, 2020, p. 26). Prieš priimant Jungtinių Tautų Visuotinę žmogaus teisių deklaraciją (toliau – VŽTD), šalies teisinės sistemos apsaugojo tik tam tikrus aspektus, kurie šiuo metu yra laikomi teise į privatumą (Krishnamurthy, 2020, p. 26). VŽTD 12 straipsnis nustatė asmens teisę į jo privatumą, šeimos gyvenimą, buitį, susirašinėjimą arba kėsinimąsi į jo garbę ir reputaciją (Visuotinė žmogaus teisių deklaracija, 1948).

VŽTD paskatino privatumo apsaugą įtraukti ir į Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvenciją (toliau – EŽTK**)** bei Tarptautinį pilietinių ir politinių teisių paktą (toliau – TPPTP) (Krishnamurthy, 2020, p. 27). EŽTK 8 straipsnis nustato, kad kiekvienas asmuo turi teisę į jo privataus ir šeimos gyvenimo gerbimą, būsto neliečiamybę ir susirašinėjimo slaptumą (Europos žmogaus teisių ir pagrindinių..., 1950). EŽTK nuostatomis vadovaujasi Europos Žmogaus Teisių Teismas (toliau – EŽTT). EŽTT pateikia praktinių išaiškinimų tam tikrais – teisės susipažinti su duomenimis ir prieštarauti jų tvarkymui, duomenų apie sveikatą ir panašiais duomenų apsaugos klausimais (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, cituota Zaleskis, 2019, p. 64).

Tarptautiniame pilietinių ir politinių teisių pakte teisė į privatumą įtvirtinta 17 straipsnyje (Tarptautinis pilietinių ir politinių teisių..., 1966). TPPTP saugo asmenis nuo savavališko ar neteisėto kišimosi į asmeninį ir šeimyninį gyvenimą, būsto neliečiamybę, susirašinėjimo slaptumą bei neteisėto kėsinimosi į asmens garbę ir orumą (Tarptautinis pilietinių ir politinių teisių…, 1966). Pakto išaiškinimas geriausiai minimas komentare, kurį JT žmogaus teisių

komitetas priėmė 1988 m. Komentaras atskleidė, kad TPPTP saugo asmenis nuo valstybės įstaigų ir privačių asmenų atliekamo jų duomenų rinkimo ir saugojimo kompiuteruose, duomenų bankuose ir kituose įrenginiuose (Zaleskis, 2019, p. 65). Atsižvelgiant į technologinių pokyčių tempą per pastaruosius trisdešimt metų ir pokyčius susijusius su privatumo įstatymų vystymusi, daugumai gali pasirodyti keista remtis tokiu senu dokumentu dėl 17 straipsnio prasmės. Tačiau, komentaras šiomis dienomis išlieka tinkamas atspirties taškas aiškinant 17 straipsnį, kadangi nustato gaires, kurių valstybės laikosi, kai pakto sutarties organas periodiškai vertina 17 str. įgyvendinimą (Krishnamurthy, 2019, p. 27).

Be to, svarbu išskirti Konvenciją dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (toliau – Konvencija Nr. 108), kadangi konvencijoje minima ne tik teisė į privatumą, tačiau ir tiesiogiai įtvirtinta duomenų apsauga. (Konvencija dėl asmenų apsaugos ryšium..., 1981). Konvencija Nr. 108 siekiama užtikrinti, jog tvarkant asmens duomenis automatizuotai, visų šalių teritorijose bus gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia teisė į privatumą (Konvencija dėl asmenų apsaugos ryšium..., 1981). Neseniai įvyko konvencijos modernizavimo procesas, kurio pagrindiniai tikslai buvo sustiprinti privatumo apsaugą skaitmeninėje arenoje bei konvencijos tolesnių veiksmų mechanismą (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba , 2018, p. 26). Darbas buvo atliktas lygiagrečiai su Europos Sąjungos (toliau – ES) duomenų apsaugos taisyklių reforma. Europos Taryba ir ES lygmens reguliavimo institucijos siekė užtikrinti abiejų teisinių sistemų nuoseklumą ir suderinamumą (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba , 2018, p. 26). Pavyzdžiui, siekiant kovoti su vis didesniu profiliavimo naudojimu internetiniame pasaulyje, konvencija Nr. 108 taip pat nustatė asmens teisę į netaikymą sprendimų, pagrįstų vien automatizuotu apdorojimu, neatsižvelgiant į pačių asmenų nuomonę (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba , 2018, p. 27).

Didieji duomenys nėra tiesiogiai paminėti prieš tai aptartuose tarptautinės teisės šaltiniuose, tačiau dėl savo pobūdžio kelti grėsmę asmens duomenims bei privatumui yra reguliuojami bendrųjų duomenų apsaugos teisės šaltinių. Didieji duomenys nėra aiškiai paminėti ir aptartoje Konvencijoje Nr. 108, tačiau šiame kontekste Europos Taryba 2017 m. išleido Asmenų apsaugos gaires dėl asmens duomenų tvarkymo didžiųjų duomenų pasaulyje (toliau – didžiųjų duomenų gairės) (De hert, Papakonstantinou, 2020, p. 8). Šios gairės aiškiai nukreiptos tiek į didžiuosius duomenis, tiek į jų analizę. Didžiųjų duomenų gairės

rekomenduoja priemones, kurių duomenų valdytojai ir duomenų tvarkytojai turėtų imtis, kad išvengtų neigiamo poveikio žmogaus orumui, žmogaus teisėms ir laisvėms, visų pirma teisei į asmens duomenų apsaugą (De Hert, Papakonstantinou, 2020, p. 8).

Be to, 2019 m. Europos Taryba gretimai išleido Dirbtinio intelekto ir duomenų apsaugos gaires (toliau – dirbtinio intelekto gairės) (Europos Taryba, 2019, cituota Papakonstantinou, 2020, p. 8). Dirbtinio intelekto gairės yra daug trumpesnis dokumentas, tačiau jo išleidimas išreiškia svarbų ryšį su 2017 m. didžiųjų duomenų gairėmis (De Hert, Papakonstantinou, 2020, p. 8). Gairėmis siekiama padėti politikos formuotojams, dirbtinio intelekto kūrėjams, gamintojams ir paslaugų teikėjams užtikrinti, kad dirbtinio intelekto programos nepakenktų teisei į asmens duomenų apsaugą (Europos Taryba, 2019, cituota De Hert, Papakonstantinou, 2020, p. 10).

Taip pat, svarbu prisiminti, jog Europos Taryba yra tarptautinė organizacija, tačiau informaciniai tekstai, tokie kaip Konvencija Nr. 108 ir BDAR yra suderinami, todėl ES valstybės narės gali tiesiogiai naudoti Europos Tarybos didžiųjų duomenų ir dirbtinio intelekto gaires. Abiejose gairėse pateiktas požiūris ir sprendimai yra suderinami su BDAR sistema, todėl ES valstybės narės gali juos taikyti užtikrindamos, jog nepažeidžia kitų ES asmens duomenų apsaugos įsipareigojimų (De Hert, Papakonstantinou, 2020, p. 11).

Taip pat dauguma duomenų apsaugos įstatymų ir toliau remiasi Ekonominio bendradarbiavimo ir plėtros organizacijos gairėmis (toliau – EBPO gairės). Šis *soft law* šaltinis puikiai atlaikė tris dešimtmečius, tačiau svarbu nepamiršti, kad, kaip ir dauguma kitų tarptautinės teisės šaltinių, buvo sukurtas ne tik prieš didžiuosius duomenis, bet ir prieš internetą, nešiojamuosius kompiuterius, GPS, išmaniuosius telefonus, planšetinius įrenginius ar kitas naujoves, kurių veikimą įgalina didieji duomenys (Kuner *et al.*, 2012, p. 49). Todėl, nustatant bendruosius principus, kuriais grindžiami duomenų apsaugos įstatymai, labai svarbu ne tik suderinti pačius įstatymus, bet ir užtikrinti jų veiksmingumą (Kuner *et al.*, 2012, p. 49).

1.3.2.2. Reguliavimas Europos Sąjungoje

Pirmiausia, pirminio šaltinio vaidmenį Sąjungos teisėje atlieka Europos Sąjungos pagrindinių teisių chartija (toliau – ES Chartija). ES Chartija tiesiogiai nemini didžiųjų duomenų sąvokos, tačiau yra laikoma bendruoju duomenų apsaugos teisės šaltiniu. ES Chartija ne tik garantuoja pagarbą asmeniniam ir šeimos gyvenimui, bet ir nustato teisę į asmens duomenų apsaugą

(Europos Sąjungos pagrindinių teisių chartija, 2012). ES Chartijos 8 straipsnyje ne tik aiškiai minima teisė į duomenų apsaugą, bet ir įtvirtinami pagrindiniai duomenų apsaugos principai. Be to, ES Chartijos 8 straipsnio 3 dalis nurodo reikalavimą, kad nepriklausoma institucija kontroliuotų šių principų įgyvendinimą (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 28). Svarbų vaidmenį duomenų apsaugos šaltinių sistemoje atlieka ir Lisabonos sutarties priėmimas, tapęs orientyru ne tik siekiant padidinti ES Chartijos privalomąjį statusą pirminės teisės lygmeniu, bet ir sustiprinti teisę į asmens duomenų apsaugą (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 28).

Antriniais duomenų apsaugos šaltiniai Sąjungoje yra 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Europos Parlamento ir Tarybos direktyva…, 2002) bei BDAR. Svarbiausias vaidmuo ES duomenų apsaugos teisėje bei reguliuojant didžiuosius duomenis tenka BDAR. Priėmus BDAR buvo modernizuoti ES duomenų apsaugos teisės aktai. Modernizacijos procesas įgalino teisės aktus tinkamai apsaugoti pagrindines teises, atsižvelgiant į skaitmeninio amžiaus ekonominius ir socialinius iššūkius (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 30). BDAR patobulino ir išplėtė pagrindinius duomenų subjektų principus ir teises, kilusius iš Duomenų apsaugos direktyvos (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 30). Reformos metais, kai kurie pramonės atstovai ir JAV mokslininkai (Tene, Polonetsky, 2013, cituota De Hert, Sajfert, 2019, p. 6) teigė, jog duomenų apsaugos principai yra pasenę dėl naujos technologinės realijos. Kiti laikėsi nuomonės, kad didieji duomenys turėtų būti traktuojami kaip bet koks kitas asmens duomenų tvarkymas. ES institucijos gynė nuomonę, kad duomenų apsaugos principai vis dar gali būti taikomi didžiųjų duomenų kontekste (De Hert, Sajfert, 2019, p. 6). Taigi, nors ir didžiųjų duomenų termino BDAR nėra, BDAR vis tiek visa apimtimi taikomas didžiųjų duomenų reguliavimui.

Be to, svarbūs ir *soft law* šaltiniai. ES Duomenų apsaugos teisėje ryškų vaidmenį atlieka ES 29 str. Darbo grupės šaltiniai. ES 29 str. Darbo grupė yra pateikusi išaiškinimus daugumos subjektų teisių, principų ar kitų reikalavimų taisyklėms (Zaleskis, 2019, p. 75). Nuomonės, gairės, rekomendacijos leidžia iš arčiau pažinti kiekvieno iš reikalavimų apimtį bei pritaikyti didžiųjų duomenų kontekste. Taip pat *soft law* šaltiniu yra laikomos ir Europos duomenų apsaugos valdybos (toliau – EDAV) gairės. EDAV gairių bendrasis tikslas yra išaiškinti Europos duomenų apsaugos teisės aktų sąlygas ir suinteresuotų duomenų apsaugos subjektų

teises ir pareigas bei užtikrinti, kad Sąjungoje būtų nuosekliai taikomas BDAR (Europos duomenų apsaugos valdyba, 2018, p. 5).

Be to, galima paminėti šaltinius, kurie ragina, jog atliekant duomenų analizę būtų užtikrinamas privatumas ir duomenų apsauga. Didžiųjų duomenų analizės reguliavimui svarbus ES veikėjų darbas dirbtinio intelekto kūrimo srityje. Europos Komisija 2018 m. įsteigė Aukšto lygio dirbtinio intelekto ekspertų grupę (De Hert, Sajfert, 2019, p. 12). Pirmaisiais įsteigimo metais Aukšto lygio dirbtinio intelekto ekspertų grupė išleido dirbtinio intelekto etikos gaires, kuriose nenagrinėjamas dirbtinio intelekto atitikimas galiojančiai reguliavimo sričiai, tačiau daugiausia dėmesio skiriama dirbtinio intelekto principų ir reikalavimų kūrimui (De Hert, Sajfert, 2019, p. 12). Tačiau, Komisija patvirtino ne tik šias gaires, bet ir nusprendė pateikti komunikatą „ Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas" (De Hert, Sajfert, 2019, p. 12). Komunikate nurodyta, jog visais dirbtinio intelekto sistemos gyvavimo ciklo etapais turi būti užtikrintas privatumas ir duomenų apsauga (De Hert, Sajfert, 2019, p. 13), taip pat komunikate BDAR įvardijamas kaip tvirtos reguliavimo sistemos dalis, kuri nustatys pasaulinį į žmogų orientuoto dirbtinio intelekto standartą (De Hert, Sajfert, 2019, p. 13).

1.3.2.3. Reguliavimas Lietuvoje

Pirmiausia, privataus gyvenimo pagrindus numato Lietuvos Respublikos Konstitucija (Lietuvos Respublikos Konstitucija, 1992). Tačiau, svarbiausias duomenų apsaugos teisės aktas Lietuvoje yra Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – LR Duomenų teisinės apsaugos įstatymas), priimtas 2018 m. LR Duomenų teisinės apsaugos įstatymas laikomas įgyvendinančiu BDAR nuostatas. Taip pat įstatymas atskleidžia ir konkretizuoja kai kurių nuostatų taikymą Lietuvos Respublikoje. Įstatymo nuostatos yra aiškesnės srityse, kuriose BDAR palieka valstybių narių nacionalinės teisės diskreciją pasirinkti. Pavyzdžiui, duomenų apsaugos įstatymo nuostatos, pažyminčios reikšmingą įtaką didžiųjų duomenų organizacijoms, gali būti siejamos su vaiko, kuriam siūlomos informacinės visuomenės paslaugos amžiumi sutikimui gauti ar kt. (Lietuvos Respublikos asmens duomenų teisinės...2018). Taip pat, svarbus Valstybinės duomenų apsaugos inspekcijos (toliau – Duomenų apsaugos inspekcija) direktoriaus įsakymu priimtas „Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sarašas"

(Duomenų tvarkymo operacijų, kurioms taikomas...,2019), kuriame nurodomos veiklos, kurios taip pat gali būti ir didžiųjų duomenų veiklos, reikalaujančios atlikti poveikio duomenų apsaugai vertinimą.

Tačiau, galima daryti išvadą, jog konkrečių šaltinių, reguliuojančių asmens duomenų apsaugą didžiųjų duomenų ar jų analizės kontekste, Lietuvos teisėje nėra. Lietuva remiasi ES nustatytu reguliavimu, o nuostatoms, kurioms ES teisės aktai palieka diskreciją nacionalinės teisės požiūriu, taiko LR Duomenų teisinės apsaugos įstatymą.

2. ES BENDRASIS DUOMENŲ APSAUGOS REGLAMENAS KAIP DIDŽIŲJŲ DUOMENŲ REGULIAVIMO ŠALTINIS

2.1. Reglamento dalykas ir tikslai

BDAR yra įtvirtintos taisyklės, susijusios su fizinių asmenų apsauga tvarkant jų asmens duomenis, ir taisyklės su laisvu asmens duomenų judėjimu. BDAR tikslas yra apsaugoti fizinių asmenų pagrindines teisės ir laisves, visų pirma jų teisę į asmens duomenų apsaugą (BDAR, 1 str). Didžiųjų duomenų rinkiniuose esant asmens duomenų atsiveria BDAR taikymo sritis. Atsižvelgiant į neapibrėžiamą didžiųjų duomenų rinkinių skaičių ir turinio įvairovę, labai tikėtina, kad asmens duomenys bus didžiųjų duomenų rinkinio dalis. Tokiu atveju visas duomenų rinkinys pateks į BDAR taisyklių taikymo sritį (Dammnann, 2016, cituota Voigt, Von dem Bussche, 2017, p. 236). Pavyzdžiui, ūkio subjektas renka ir analizuoja duomenis apie savo gamybos apimtį. Duomenų rinkinyje yra informacijos apie tai, kiek produktų skirtingos įmonės mašinos pagamina per valandą (Voigt, Von dem Bussche, 2017, p. 236). Duomenų rinkimas kartu su papildoma informacija, kaip darbuotojų pamainų grafikai leidžia įmonei nustatyti, kuris asmuo tuo metu valdė mašiną, ir taip padaryti išvadas apie jo darbo rezultatus (Voigt, Von dem Bussche, 2017, p. 236). Šiuo atveju įmonė gali panaudoti duomenų rinkinį norėdama gauti informacijos apie savo darbuotojų produktyvumą. Tokiu atveju duomenų rinkinį galima susieti su duomenimis apie asmenį, todėl jo apsaugai taikomos BDAR įtvirtintos taisyklės (Voigt, Von dem Bussche, 2017, p. 236). BDAR tikslas būtų užtikrinti šių asmenų teisių ir laisvių apsaugą.

Be to, BDAR įtvirtinomis taisyklėmis siekiama apsaugoti tik asmens duomenis. BDAR 4 straipsnyje apibrėžiama asmens duomenų sąvoka. Asmens duomenys yra bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima tiesiogiai ar netiesiogiai nustatyti (BDAR, 4 str.). Asmens tapatybė gali būti nustatyta pagal akivaizdžius identifikatorius, kaip asmens vardas, vietovės duomenys ar aiškus internetinio tinklalapio vartotojo vardas (Zaleskis, 2019, p. 91). Taip pat tapatybę galima nustatyti ir pagal mažiau aiškius identifikatorius, kaip IP adresas, asmens kodas ar slapukų identifikatorius (BDAR preambulės 30 punktas, cituota Zaleskis, 2019, p. 95).

Fizinis asmuo, kurio asmens duomenys saugomi remiantis BDAR taisyklėmis yra vadinamas duomenų subjektu (BDAR, 4 str.). Minėtuoju pavyzdžiu dėl produktyvumo darbo

aplinkoje duomenų subjektu būtų įmonės darbuotojas, tačiau žvelgiant į platų asmens duomenų panaudojimo spektrą, duomenų subjektu didžiųjų duomenų kontekste gali būti bet kas, kaip, pavyzdžiui, asmuo, besinaudojantis tinklalapiu „Facebook“, „Netflix“, „Yahoo“ ir daugelis kitų atvejų, kuomet duomenų valdytojas savo veiklą grindžia didžiaisiais duomenimis ir (ar) jų analize.

2.2. Specialiųjų kategorijų asmens duomenys

Asmens duomenys, kurie pagal savo pobūdį yra neskelbtini pagrindinių teisių ir laisvių atžvilgiu, turi išskirtinę apsaugos garantiją. Šių kategorijų duomenų paskleidimas ar nutekinimas gali potencialiai sukelti didžiausią žalą (Ohm, 2015, cituota Zarsky, 2017, p. 1012). BDAR 9 str. 1 dalis nustato, kad specialiųjų kategorijų duomenų tvarkymas yra draudžiamas (BDAR, 9 str.). Specialiųjų kategorijų asmens duomenys apima rasinę ar etninę asmens kilmę, politines pažiūras, asmens religiją ir tikėjimą, genetinę informaciją ar sveikatos būklę (BDAR, 9 str.). Tačiau, šis draudimas turi ir išimčių, įskaitant aiškų duomenų subjekto sutikimą, duomenų subjekto savanorišką tokių kategorijų duomenų paskelbimą internete ir kitus būdus, įtvirtintus BDAR 9 str. 2 dalyje (BDAR, 9 str.). Be to, norint tvarkyti specialiųjų kategorijų duomenis dideliu mastu, gali būti reikalingas poveikio duomenų apsaugai vertinimas (BDAR, 35 str.), duomenų apsaugos pareigūno skyrimas (BDAR, 37 str.) bei tinkamų techninių ir organizacinių priemonių įgyvendinimas, pagrįstas didelės rizikos perdirbimo situacija (Voigt, Von dem Bussche, 2017, p. 116).

Didžiųjų duomenų analizė paprastai neskiria paprastųjų ir specialiųjų kategorijų asmens duomenų, todėl analizuojant didžiųjų duomenų rinkinius sunku apdoroti duomenis laikantis BDAR nustatytų taisyklių, pradedant nuo specialiųjų kategorijų duomenų atskirties (Ajibade, 2018, p. 41). Analizė, kuri remiasi įprastomis kategorijomis, gali gana greitai tapti susijusi ir su specialiomis kategorijomis (Ohm, 2015, cituota Zarsky, 2017, p. 1013). Pavyzdžiui, duomenis apie asmens sveikatą, rasę ar seksualinę orientaciją galima išskaičiuoti iš apsipirkimo duomenų bazės, kuomet duomenų analizė perėjo iš įprastos duomenų kategorijos į specialią (Ajibade, 2018, p. 41). Todėl, būtinybė atskirti „įprastų“ ir „specialių“ kategorijų apdorojimą gali apsunkinti didžiųjų duomenų procesus, kurie gali netyčia pereiti iš vienos kategorijos į kitą, o kiekvienam iš jų reikia taikyti kitokį teisinių taisyklių rinkinį (Zarsky, 2017, p. 1013).

2.3. Teritorinis taikymas

Šiomis dienomis dėl technologijų pažangos ir plataus interneto naudojimo ES piliečių asmens duomenys tvarkomi ne tik ES, bet ir už jos ribų. Priėmus BDAR, pakeitusiu Duomenų apsaugos direktyvą, ES teisės aktų leidėjai peržengė teritoriškumo principą. Galimybė taikyti BDAR nuostatas peržengiant teritoriškumą reikalauja gana tvirto ryšio tarp veiksmo ir ES teritorijos (De Hert, Czerniawski, 2016, p. 1). BDAR įtvirtino platesnę teritorinę taikymo sritį nei buvusi Duomenų apsaugos direktyva. Platesnė teritorinio taikymo apimtis yra būdas užtikrinti veiksmingą duomenų apsaugos įstatymų vykdymą interneto amžiuje (De Hert, Czerniawski, 2016, p. 2). Pakeitimas atitinka naujausius ESTT nuosprendžius ir neprieštarauja modernizuotai konvencijai Nr. 108 (De Hert, Czerniawski, 2016, p. 2). Be to, BDAR jurisdikcijos taikymo sritis grindžiama pagrįstais pagrindais, atsižvelgiant į galimus jurisdikcijos konfliktus ir ES duomenų apsaugos įstatymų teisėtumą (De Hert, Czerniawski, 2016, p. 2).

Teritorinė taikymo sritis išdėstyta BDAR 3 straipsnyje. Pirma, reglamentas taikomas asmens duomenų tvarkymui, kai asmens duomenis Sąjungoje tvarko duomenų valdytojo arba duomenų tvarkytojo buveinė, vykdydama savo veiklą, neatsižvelgiant į tai, ar duomenys tvarkomi Sąjungoje, ar ne (BDAR, 3 str.). Nuostata pasižymi įsisteigimo principu, pagal kurį teisės pasirinkimas priklauso nuo to, kur yra įsisteigęs valdytojas ar tvarkytojas. Asmens duomenų tvarkymo vieta nėra lemiamas veiksnys, jei valdytojas ar tvarkytojas Sąjungoje turi buveinę (Voigt, Von dem Bussche, 2017, p. 22). Šią nuostatą BDAR išplėsti paskatino ESTT sprendimas byloje *Google Spain SL, Google Inc v. Agencia Española de Protección de Datos, Mario Costeja Gonzále* (toliau – *Google Spain* sprendimas), kurio pagrindu ir Komisijos idėjomis duomenų valdytojui nebūtina tvarkyti duomenų Europos Sąjungoje norint patekti į jos jurisdikciją (De Hert, Czerniawski, 2016, p. 2). Atsižvelgiant į bylos faktus, bendrovė „Google Inc“ įsikūrusi JAV, tačiau generuojamų reklaminių pranešimų vietoms parduoti tinklalapyje „Google“ pasitelkia savo dukterinę bendrovę „Google Spain“. Bendrovė „Google Spain“ nevykdo jokios tvarkymo veiklos, tačiau iš esmės prisideda prie bendrovės ekonominės sėkmės, plėtoja santykius su klientais ir dėl to turi nemažą stabilumo laipsnį (Voigt, Von dem Bussche, 2017, p. 24). ESTT teigė, jog svarbu ne tai, kad atitinkamą duomenų tvarkymą atliktų „pats“ padalinys, o tai, kad tvarkymas būtų atliekamas šiam padaliniui „vykdant veiklą“

(*Google Spain ir Google,* 2014, 52 punktas). Sprendimas buvo priimtas galiojant Duomenų apsaugos direktyvai. Duomenų apsaugos direktyvos nuostatos tiesiogiai ir aiškiai neįtvirtino galimybės vadovautis tokia taikymo sritimi, tačiau ESTT laikėsi pozicijos, kad norint pasiekti žmogaus teisių tikslus direktyvos nuostatos turi būti aiškinamos plačiai. Požiūris buvo teisingas, tačiau išplėtė teisines nuostatas (De Hert, Czerniawski, 2016, p. 2). Sprendimas pridėjo ekstrateritorinius įgaliojimus į iš esmės tik teritoriniu pagrindu pagrįstą Duomenų apsaugos direktyvos taikymo sritį (De Hert, Czerniawski, 2016, p. 13). Todėl, šis aiškinimas paskatino tiesioginę formuluotę BDAR.

BDAR 3 str. 2 dalį rengėjai laiko vienu svarbesnių reformos pasiekimų (De Hert, Czerniawski, 2016, p. 2). Nuostata leidžia į reglamento taikymo sritį įtraukti duomenų valdytojus ar tvarkytojus, įsisteigusius už Sąjungos ribų, kai jie a) siūlo prekes ar palaugas ES duomenų subjektui, neatsižvelgiant į tai, ar reikalaujamas mokėjimas; b) stebi duomenų subjektų elgesį tiek, kiek jų elgesys vyksta Europos Sąjungoje (BDAR, 3 str.). Šių dviejų punktų atveju nėra „buveinės“ kriterijaus, tačiau reikalaujamas stiprus ryšys tarp veiksmo ir ES (De Hert, Czerniawski, 2016, p. 2).

ES nepriklausantys subjektai yra įtraukiami į BDAR, kai jie siūlo prekes ar paslaugas ES duomenų subjektams (De Hert, Czerniawski, 2016, p. 9). Pavyzdžiui, norint nustatyti, ar prekės ar paslaugos yra skirtos vidaus rinkai, reikėtų išsiaiškinti, ar duomenų vadytojas ar tvarkytojas konkrečiai numato teikti paslaugas vienoje ar daugiau ES valstybių narių. Atitinkama įmonė turi ketinti kreiptis į ES vartotojus (BDAR preambulės 23 punktas, cituota Voigt, Von dem Bussche, 2017, p. 26). Vien tik prieigos prie interneto, el. pašto adreso ar kitos kontaktinės informacijos ar kalbos, paprastai vartojamos trečioje šalyje kurioje įsteigta įmonė, vartojimo nepakanka tokiam ketinimui išreikšti (BDAR preambulės 23 punktas). Tačiau indeksai, skirti ES subjektams gali būti tokie, kaip kalbos, paprastai vartojamos vienoje ar daugiau ES valstybių narių, vartojimas, valiutos nurodymas, ES klientų paminėjimas, pristatymo galimybės nurodymas į vieną ar daugiau ES valstybių narių, svetainės domeno vardas, nurodantis vieną ar daugiau ES valstybių narių, pavyzdžiui, „xxx.com/de”, „xxx.es” ar kt. (Voigt, Von dem Bussche, 2017, p. 26).

Be to, siekiant suprasti to paties straipsnio 2 dalies b punktą, svarbu paminėti, ką reiškia straipsnyje įtvirtinta „stebėsena“ (BDAR, 3 str.). Šis punktas skirtas trečiųjų šalių socialinių tinklų operatoriams, internetiniams paslaugų teikėjams, kaip el. pašto abonentams, paieškos sistemų ir svetainių operatoriams, kurių didžioji dauguma sistemingai stebi interneto vartotojų

elgesį (De Hert, Czerniawski, 2016, p. 9). Atsižvelgiant į nuostatos frazę: „tiek, kiek jų elgesys vyksta Europos Sąjungoje" akivaizdu, jog iš teritorinės taikymo srities pašalinamos situacijos, kai ryšys tarp ES valstybės narės ir duomenų valdytojo veiksmų yra gana silpnas (De Hert, Czerniawski, 2016, p. 9).

Atsižvelgiant į šių nuostatų sąsają su didžiųjų duomenų verslais, akvaizdu, jog esant vienos iš trijų išvardintų sąlygų buvimui, didžiųjų duomenų organizacijos, kurių veikla apima asmens duomenis, patenka į BDAR teritorinę taikymo sritį bei privalo laikytis visų šio teisės akto nustatytų taisyklių. BDAR teritorinė taikymo sritis labai plati. Įmonės, atliekančios tik didžiųjų duomenų analizę, nors ir pačios nerinkdamos asmens duomenų taip pat turi laikytis BDAR nustatytų sąlygų.

2.4. Duomenų valdytojas ir duomenų tvarkytojas

BDAR 4 str. 7 punktas nustato, jog duomenų valdytoju yra laikomas a) fizinis ar juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri b) viena ar drauge su kitais, c) nustato duomenų tvarkymo tikslus ir priemones (BDAR, 4 str.). Panašiai duomenų valdytojas apibrėžiamas konvencijoje Nr. 108 bei EBPO privatumo gairėse (Zaleskis, 2019, p. 99). Duomenų valdytojui tenka pagrindinė atsakomybė – įgyvendinti visus nustatytus reikalavimus (Zaleskis, 2019, p. 99). BDAR 5 str. 2 d. nustato, jog remiantis atsakomybės principu, duomenų valdytojas yra atsakingas, kad būtų laikomasi duomenų apsaugos teisės reikalavimų, ir turėtų sugebėti įrodyti, kad jų laikomasi (Zaleskis, 2019, p. 99).

Be to, BDAR 26 str. 1 d. nustato, jog, kai du ar daugiau duomenų valdytojų kartu nustato duomenų tvarkymo tikslus ir priemones, jie yra bendri duomenų valdytojai (BDAR, 26 str.). Įstatymų leidėjas siekė, kad atsakomybė būtų aiškiai paskirstyta, todėl šiame straipsnyje įvedė bendrų duomenų valdytojų sąvoką (Voigt, Von dem Bussche, 2017, p. 18). Bendras valdymas gali būti įvairių formų, pavyzdžiui, dalintis visais tvarkymo tikslais ar tik dalinai (Voigt, Von dem Bussche, 2017, p. 18).

BDAR 4 str. 8 punkte apibrėžiama duomenų tvarkytojo sąvoka. Duomenų tvarkytojas – tai fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis (BDAR, 4 str.). Duomenų tvarkytojo buvimas priklauso nuo duomenų valdytojo priimto sprendimo. Duomenų valdytojas gali a) tvarkyti duomenis savo organizacijoje; b) perduoti visą ar dalį duomenų tvarkymo veiklos išorės

organizacijai (ES 29 str. Darbo grupė, 2010, cituota Voigt, Von dem Bussche, 2017, p. 20). Duomenų tvarkytojas turi atitikti dvi pagrindines sąlygas: a) būti nuo duomenų tvarkytojo nepriklausomas, savarankiškas fizinis ar juridinis asmuo; b) tvarkyti asmens duomenis duomenų valdytojo vardu (ES 29 str. Darbo grupė, cituota Zaleskis, 2019, p. 102). Pavyzdžiui, bendrovės, kurios duomenys sudaro didžiųjų duomenų rinkinius, direktorius nusprendžia, kad debesijos technologijų įmonė tvarkytų jo įmonės klientų duomenis. Duomenis patikėjusi įmonė lieka duomenų valdytojas, o debesijos technologijomis užsiimanti įmonė tampa tvarkytoju. Pagal tarpusavio susitarimą, debesijos technologijų įmonė tvarko ir saugo duomenis bendrovės, pateikusios duomenis saugoti debesyje, tikslais. Debesijos technologijų įmonė yra duomenų valdytojo paslaugos teikėjas ir tvarko asmens duomenis valdytojo vardu (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 108).

Atsižvelgiant į sudėtingas didžiųjų duomenų programas, kurioms veikiant asmens duomenys gaunami iš skirtingų šaltinių ir subjektų, gali būti sunku nustatyti, kas bus atsakingas už duomenų apsaugą ir duomenų subjektų prašymus (Werkmeister, Brandt, 2016, cituota Voigt, Von dem Bussche, 2017, p. 237). Paprastai, kai tam tikros organizacijos užsako duomenų analizę, kurią atlieka įmonės, kurios specializuojasi didžiųjų duomenų srityje, užsakančios analizę įmonės ir nustato duomenų tvarkymo būdus, tikslus ir yra laikomos duomenų valdytojais, o įmonės atliekančios analizę veikia pagal savo klientų nurodymus kaip duomenų tvarkytojai (Werkmeister, Brandt, 2016, cituota Voigt, Von dem Bussche, 2017, p. 237). Tačiau, duomenų tvarkyme dalyvaujančių subjektų vaidmenys turi būti nustatomi kiekvienu atveju atskirai, nes, kaip ir minėta prieš tai, keli subjektai gali būti laikomi duomenų valdytojais, jei jie nusprendžia dėl duomenų tvarkymo tikslų ir priemonių (Voigt, Von dem Bussche, 2017, p. 237). Todėl, perkeliant didžiųjų duomenų analizę kitoms įmonėms, svarbu atidžiai apsvarstyti, kur iš tikrųjų yra asmens duomenų tvarkymo kontrolė, kadangi tai turės reikšmės ne tik už atitikimą, bet ir atsakomybę (Information Commissioner‘s Office, 2017, p. 57).

3. ES BENDROJO DUOMENŲ APSAUGOS REGLAMENTO PRINCIPAI, TAIKOMI DIDŽIŲJŲ DUOMENŲ REGULIAVIMUI

3.1. Teisėtumo, sąžiningumo ir skaidrumo principas

BDAR 5 str. 1 d. a p. nustato, jog duomenų subjekto atžvilgiu, asmens duomenys turi būti tvarkomi teisėtai, sąžiningai ir skaidriai (BDAR, 5 str.). Principas kyla ne tik iš BDAR, bet ir iš konvencijos Nr. 108. Duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principas yra svarbiausias, plačiausios apimties ir abstrakčiausias duomenų apsaugos teisės principas (Zaleskis, 2019, p. 113). Be to, teisėtumą, sąžiningumą ir skaidrumą galima laikyti atskirais duomenų apsaugos teisės principais (Zaleskis, 2019, p. 113).

3.1.1. Teisėtumas

Pirmiausia, teisėtumo principas reiškia atitiktį visiems duomenų apsaugos teisės norminiams šaltiniams, įskaitant tarptautinės, ES, nacionalinės duomenų apsaugos teisės nuostatas. Todėl, nors duomenų tvarkymo teisėtumas yra aiškiai apibrėžtas BDAR, vien BDAR taikymo apimtimi neapsiribojama (Zaleskis, 2019, p. 114).

Be to, teisėtumui taip pat gali reikėti laikytis papročių, elgesio kodeksų ir sutartinių susitarimų (Finck, Biega 2021, p. 12). Todėl, didžiųjų duomenų analizės kontekste, nors pasikliovimas tokiais elementais priklauso nuo kiekvieno konkretaus atvejo, derėtų paminėti, jog gali prireikti vadovautis ne tik pirminės teisės įstatymų normomis, tačiau atsižvelgti ir į neprivalomus dirbtinio intelekto etikos kodeksus (Finck, Biega 2021, p. 13).

3.1.1.1. Reikalavimas turėti teisėtą duomenų tvarkymo pagrindą

BDAR 6 str. nustato, jog norint, kad duomenų tvarkymas būtų teisėtas, jis turi atitikti teisėto duomenų tvarkymo pagrindus, ir tai gali būti: a) duomenų subjekto sutikimas; b) sutartis su duomenų subjektu, c) duomenų valdytojui taikoma teisinė prievolė; d) gyvybiniai fizinio asmens interesai; e) užduotis viešojo intereso labui arba viešosios valdžios funkcijos, f) teisėti duomenų valdytojo ar trečiosios šalies interesai (BDAR, 6 str.). Darbe išsamiai nagrinėjamas duomenų subjekto sutikimas.

BDAR 4 str. 11 punktas nustato, jog duomenų subjekto sutikimas – tai 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 (BDAR, 4 str.). Paprastai tariant, duomenų subjektai turi aiškiai suprasti, ką organizacija siekia daryti su jų duomenimis, ir turi būti aiški nuoroda, kad jie su tuo sutinka.

Sutikimo sąvokos elementas „laisvas“ reiškia, kad duomenų subjektai turi realų pasirinkimą ir kontrolę (ES 29 str. Darbo grupė, 2017, p. 5). ES 29 str. Darbo grupė pažymi, kad, jeigu duomenų subjektas neturi realaus pasirinkimo, jaučiasi priverstas sutikti arba patirtų neigiamų pasekmių, jei sutikimo neduotų, toks sutikimas negalioja (ES 29 str. Darbo grupė, 2017, p. 5). Duomenų subjekto valios klausimas pasižymėjo 2018 m. gegužės 25 d. ,,None of Your Business'' skunde dėl ,,Facebook Ireland Ltd" (*None of Your Business* skundas dėl *Facebook Ireland Ltd.,* 2018). Duomenų valdytojas socialiniame tinklalapyje ,,Facebook" patalpino daugybę išokančių langų ir priminimų, aiškiai parodydamas, kad sutikimas su aukščiau pateiktomis sąlygomis yra vienintelis būdas, kuriuo duomenų subjektas gali išlaikyti preigą prie savo paskyros ir toliau naudotis ,,Facebook" paslaugomis (*None of Your Business* skundas dėl *Facebook Ireland Ltd,* 2018). Išaiškinta, jog duomenų subjekto nesutikimas lemtų prieigos praradimą prie asmeninės informacijos. Duomenų subjektas privalėjo sutikti su visomis nuorodomis, tam, kad išsaugotų savo prieigą prie socialinio tinklalapio paskyros, todėl, laikoma, jog duomenų valdytojas sutikimą gavo prieš duomenų subjekto valią (*None of Your Business* skundas dėl *Facebook Ireland Ltd.,* 2018).

BDAR taip pat nurodoma, kad sutikimas turi būti nedviprasmiškas, konkretus bei turi būti aiškus patvirtinantis veiksmas, kaip pavyzdžiui, pažymėti langelį interneto svetainėje arba pasirinkti konkrečius informacinės visuomenės paslaugų parametrus (BDAR preambulės 32 punktas).

Taip pat duomenų valdytojas turi sugebėti įrodyti, kad sutikimas buvo duotas, o duomenų subjektas turi turėti galimybę atšaukti šį sutikimą (BDAR, 7 str.). Įrodinėjimo pareiga gali tapti ypač aktuali, kai sutikimas gautas internetu. Norint gauti sutikimą internete, praktikoje gali būti taikoma dviejų žingsnių procedūra (Voigt, Von dem Bussche, 2017, p. 93). Pavyzdžiui, pirmiausia duomenų subjektas pareikš sutikimą paprašius įvesti savo el. pašto adresą. Antrajame etape duomenų subjektas gauna patvirtinimo el. laišką su suasmeninta nuoroda, kurią subjektas turi atidaryti, kad duomenų valdytojas patvirtintų galutinį sutikimą (Voigt, Von dem Bussche, 2017, p. 93). Tokiu būdu duomenų valdytojas gali įrodyti, kad gavo sutikimą, o

duomenų subjektas sutiko. Patvirtinimo el. laiškas leidžia atmesti trečiųjų šalių piktnaudžiavimą duomenų subjektų el. pašto adresu (Voigt, Von dem Bussche, 2017, p. 93).

3.1.2. Sąžiningumas

BDAR, taip pat ir kiti duomenų apsaugos teisės aktai reikalauja laikytis ir sąžiningumo principo. BDAR 5 str. 1. a. punktas nustato, jog duomenų valdytojai turi laikytis sąžiningumo principo duomenų subjekto atžvilgiu (BDAR, 5 str.), tačiau konkretus principo turinys nėra apibrėžtas nei duomenų apsaugos teisėje, nei kitose teisės srityse (Zaleskis, 2019, p. 114). Įstatymų leidėjai palieka pasirinkimą sąžiningumą vertinti kiekvienu konkrečiu atveju ir atsižvelgiant į aplinkybes (Zaleskis, 2019, p. 114). Sąžiningumas reikalauja atidumo, rūpestingumo ir draudžia piktnaudžiauti teise (Zaleskis, 2019, p. 115). Šis principas pirmiausia reglamentuoja duomenų valdytojo ir duomenų subjekto santykius (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2018, p. 120).

Duomenų valdytojai turi pareigą pranešti subjektams, kad jie tvarkys duomenis teisėtai ir skaidriai bei turi sugebėti įrodyti, kad tvarkymo operacijos atitinka BDAR nuostatas. Apdorojimo operacijos neturi būti atliekamos slaptai, o duomenų subjektai turi žinoti apie galimą riziką (Europos Sąjungos pagrindinių teisių agentūra; Europos Taryba, 2018, p. 118). Organizacijos, kad ir kokia sudėtinga būtų analizė, turi būti sąžiningos duomenų subjektų atžvilgiu ir prireikus gauti duomenų subjektų sutikimą. Taip pat, kai atliekama didžiųjų duomenų analizė, organizacijoms tenka atsakomybė informuoti duomenų subjektą apie tikslą ir apdorojimo pasekmes (Gold, 2014, cituota Ajibade, 2018, p. 25). Be to, sąžiningumas gali būti siejamas ir su bet kokia didžiųjų duomenų analizės veikla, įskaitant tai, jog analizė yra turi būti vykdoma sąžiningai ir jos metu gauti sprendimai negali pasižymėti diskriminuojančiu pobūdžiu (Veale, Edwards, 2018, p. 403).

Be to, sąžiningumo principas numato proporcingumą kaip išankstinę sąlygą, kadangi tikimasi, jog tvarkant duomenis, duomenų valdytojas atsižvelgs į duomenų subjekto interesus, kad išvengtų jų įsibrovimo nereikalingu, nepagrįstu ar pernelyg dideliu būdu (Bygrave, Schartum, 2009, cituota Ajibade 2018, p. 24). Paprastai tariant, didžiųjų duomenų valdytojai visuomet turi apsvarstyti, ar tam tikras didžiųjų duomenų tvarkymas, panaudojimas yra su derinamas su asmenų lūkesčiais.

3.1.3. Skaidrumas

Didieji duomenys neatsiejami ir nuo skaidrumo principo laikymosi. Skaidrumas, kai duomenų valdytojai jį užtikrina, įgalina duomenų subjektus laikyti duomenų valdytojus ir duomenų tvarkytojus atskaitingais ir kontroliuoti savo asmens duomenis (ES 29 str. Darbo grupė, 2017, p. 5).

BDAR 2 skyriuje išsamiai aprašoma duomenų subjekto teisė į informaciją. Taip pat aprašoma prieiga prie asmens duomenų, ir tai yra aiškiai nurodoma BDAR 13-15 straipsniuose. BDAR 13 ir 14 str. yra duomenų valdytojams nustatytos pareigos pranešti, o 15 straipsnis numato teisę susipažinti su informacija viso tvarkymo metu (Selbst, Powles, 2017, p. 2).

Didžiųjų duomenų analizės sudėtingumas gali reikšti, kad asmenims, kurių duomenys naudojami, duomenų tvarkymas yra akivaizdžiai nematomas. Duomenų subjektams gali būti neaišku, ar renkami jų duomenys, kaip, pavyzdžiui, mobiliojo telefono lokacija. Taip pat gali kilti klausimų, kaip ir kokiu būdu duomenys yra apdorojami, pavyzdžiui, kai jų paieškos rezultatai filtruojami remiantis algoritmais (Information Commissioner‘s Office, 2017, p. 27). Akivaizdu, kad norint užtikrinti asmenų žinomumą apie su asmenų duomenimis vykstančius procesus, organizacijos privalo įgyvendinti skaidrumo principą. Organizacijos turi skaidriai ir lengvai prieinama forma skelbti duomenų apsaugos politiką. Paprastomis piktogramomis svetainėje galima paaiškinti, kaip ir kas tvarkys asmens duomenis bei kas bus už tai atsakingas (Jourová, 2016, p. 3). Pavyzdžiui, „Google“ turi ilgą aprašymą. Pirmiausia, informuoja vartotojus, kad duomenys renkami norint sukurti geresnes paslaugas, prieš pateikdami pavyzdžius, ką tai reiškia. Taip pat informuoja savo vartotojus, kad naudoja automatizuotas sistemas, analizuojančias jų turinį, kad pateiktų pritaikytus paieškos rezultatus ar skelbimus (Finck, Biega, 2021, p. 8).

3.2. Duomenų tikslo apribojimo principas

Tikslo apribojimo principas yra įtvirtintas ne tik BDAR, tačiau ir ES Chartijoje. BDAR 5 str. 1 d. b punktas nustato, jog duomenys turi būti renkami a) nustatytais, b) aiškiai apibrėžtais bei c) teisėtais tikslais ir d) toliau netvarkomi su tais tikslais nesuderinamu būdu (BDAR, 5 str.). Paprastai tariant, principas įpareigoja duomenų valdytojus tiksliai apibrėžti, kokių duomenų jiems reikia bei neskatina kaupti asmens duomenis spekuliaciniam naudojimui ateityje (Finck,

Biega, 2021, p. 11). Svarbu tai, kad tikslą rekėtų apibrėžti prieš pradedant rinkti duomenis (ar bet kokį kitą duomenų tvarkymą) (Finck, Biega, 2021, p. 11).

Pirma, duomenų tvarkymo tikslai yra nustatyti, kai yra apibrėžti pakankamai tam, kad būtų galima įgyvendinti kitus duomenų apsaugos teisės reikalavimus ir suprasti duomenų tvarkymo operacijų apimtį (Zaleskis, 2019, p. 118). ES 29 str. Darbo grupės nuomone, bendri teiginiai, kaip „gerinti vartotojo patirtį“, „komerciniais tikslais“ ar „reklamai“ paprastai nėra pakankamai konkretūs (ES 29 str. Darbo grupė, 2013, cituota Finck, Biega, 2021, p. 11). Šis reikalavimas pasižymi didele svarba, o, pavyzdžiui, rekomendacijų algoritmais paprastai siekiama daugiau patobulinti, o ne teikti konkrečią paslaugą, todėl, didžiųjų duomenų organizacijoms apribrėžiant tikslus realu neišlaikyti specifikacijos testo (Finck, Biega, 2021, p. 11). Antra, tikslai turi būti aiškiai apibrėžti, t.y. atskleisti, paaiškinti ir išreikšti suprantama forma (Zaleskis, 2019, p. 119). Svarbu tai, kad tikslai turi būti konkrečiai apibrėžti, tačiau taip pat turi būti suprantami duomenų subjektams. Norint pasiekti abu tikslus, rekomenduojami daugiasluoksniai pranešimai, nes jie gali pateikti bendrą paaiškinimą ir pakankamą išsamumą (ES 29 str. Darbo grupė, 2013 cituota Finck, Biega, 2021, p. 12). Trečia, tikslo teisėtumas įpareigoja tvarkyti duomenis pagal galiojančius įstatymus, pavyzdžiui, nediskriminavimo, baudžiamąją ar darbo teisę. Teisėtumui taip pat reikėtų laikytis papročių, elgesio kodeksų, etikos kodeksų ar sutartinių susitarimų (ES 29 str. Darbo grupė, 2017 cituota Finck, Biega, 2021, p. 12). Ketvirta, kaip ir minėta, duomenys negali būti tvarkomi su nustatytais tikslais nesuderinamu būdu (BDAR, 5 str.).

Draudimo tvarkyti duomenis su tikslais nesuderinamu būdu paprastas pavyzdys gali būti sveikatos draudimo kompanija, kuri renka pacientų duomenis, kad turint tinkamą klientų duomenų bazę būtų galima atlikti kompensacijas už vaistus, gydymą, terapiją (Custers, Uršič, 2016, p. 5). Tikslo nesuderinamumas pasižymėtų tuo atveju, jei ta pati draudimo bendrovė pradėtų naudoti duomenis siekiant išanalizuoti asmenų rizikos grupes, kaip, pavyzdžiui, siekiant nustatyti šias grupes ir pagal tai pritaikyti draudimo įmokų dydį. Tokiu atveju įmonė panaudos duomenis kitiems tikslams (Loshin, 2011, cituota Custers, Uršič, 2016, p. 5). Tačiau, šiuo atveju pasireiškia galimybė siekti asmens sutikimo dėl pakartotinio asmens duomenų panaudojimo (Custers, Uršič, 2016, p. 5).

Be to, tikslo apribojimo principas pasižymi ir tam tikromis išimtimis, reiškiančiomis, jog tolesnis asmens duomenų tvarkymas mokslo, istoriniais ar statistikos tikslais laikomas atitinkančiu tikslo ribojimo principą, laikantis atitinkamų apsaugos priemonių (BDAR, 5 str.).

Didžiųjų duomenų programos, susijusios su tolesniu duomenų tvarkymu mokslo ir statistikos tikslais nesusiduria su kliūtimis jei išlaikomos tinkamos duomenų subjektų apsaugos priemonės. Apsaugos priemonių nustatymas, akivaizdu, jog reikalauja didžiųjų duomenų valdytojų išteklių ir pastangų (Forgó *et. al.*, 2017, p. 40). Tačiau, tikslo apribojimo principo išimtys nepriskiriamos prie nuostatų, nesuderinamų su didžiųjų duomenų prigimtimi bei gali būti laikomos sąmoninga BDAR rengėjų pastanga leisti naudoti didžiuosius duomenis (Ajibade, 2018, p. 34).

Tikslo apribojimo principo principas plačiai nagrinėtas ir technologijų specialistų bendruomenės. Daugelis komentatorių ir pranešėjų pažymi, jog tikslo apribojimas aiškiai riboja didžiųjų duomenų analizės perspektyvas (Hildebrandt, 2013, cituota Zarsky, 2017, p. 1005). Didžiųjų duomenų prigimtis reikalauja naudoti metodus ir modelius, į kuriuos, nei duomenų valdytojas, nei duomenų subjektas neatsižvelgė ar net neįsivaizdavo rinkimo metu (Zarsky, 2017, p. 1006). Norint įgyvendinti tikslo specifikavimo taisyklę, turima informuoti duomenų subjektą apie būsimas tvarkymo formas, akivaizdžiai stebėti savo praktiką ir užtikrinti, jog neviršytina leistina analizės sritis (Zarsky, 2017, p. 1006). Žinoma, kaip ir minėta draudimo bendrovės pavyzdžiu, tai neužkerta kelio duomenų panaudojimui kitiems tikslams, kadangi pasireiškia galimybė gauti pakartotinį asmens sutikimą. Tačiau, kita vertus, tai gali apsunkinti didžiųjų duomenų analize užssimančių duomenų valdytojų veiklą, kadangi didžiųjų duomenų analizė visada linkusi atrasti naujus tikslus, tad sutikimą galimai reikės gauti ne vieną kartą, o sutikimui taikomi griežti BDAR reikalavimai. Be to, didžiųjų duomenų įmonės negali apriboti duomenų subjekto atšaukti sutikimą, kai bus nustatyta pakartotinė jo asmens duomenų paskirtis (Ajibade, D. 2018, p. 34). Atšaukimas reikštų, kad duomenų, kurie yra didžiųjų duomenų analizės modelio dalis, kurių neįmanoma anonimizuoti, dėl kurių tvarkymo asmens sutikimas buvo atšauktas, tvarkyti nebegalima (Finck, Biega, 2021, p. 23). Problema kyla tame, jog dar vis nėra nustatyta kaip pritaikyti BDAR 7 str. 3 dalį mašininiam mokymuisi. Kompiuterių mokslininkai tik neseniai pradėjo kurti sprendimus, kaip efektyviai ištrinti atskirus duomenų taškus iš apmokyto mašininio mokymosi, ir tam dar reikalingi tolimesni tyrimai (Ginart *et al.*, 2019, cituota Finck, Biega, 2021, p. 24).

3.3. Duomenų kiekio mažinimo principas

BDAR 5 str. 1 d. c punktas reikalauja, kad asmens duomenys būtų adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (BDAR, 5 str.). Duomenų kiekio mažinimo principas yra glaudžiai susijęs su duomenų tvarkymo tikslo apribojimo principu (Zaleskis, 2019, p. 121). Tačiau, skirtingai nuo „tikslo specifikacijos", šis principas nėra aiškiai paminėtas ES Chartijoje (Zarsky, 2017, p. 1009). Kad atitiktų duomenų kiekio mažinimo principą, duomenų tvarkymas turi atitikti tris elementus:

1. Būtinumas - duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis (Zaleskis, 2019, p. 122).
2. Tinkamumas - duomenys gali būti reikšmingi duomenų tvarkymo tikslams pasiekti. Draudžiama rinkti ir tvarkyti duomenis, kurie nėra niekaip susiję su duomenų valdytojo veikla ir jo tikslais (Zaleskis, 2019, p. 122).
3. Adekvatumas - tvarkomi duomenys turi būti proporcingi duomenų tvarkymo tikslams (Zaleskis, 2019, p. 122).

Atsižvelgiant į sąsają su kitais BDAR principais, duomenų kiekio mažinimo principas yra papildomas saugojimo trukmės apribojimo principu. BDAR 5 str. 1 d. e punktas nustato, jog duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi (BDAR, 5 str.). Be to, duomenų kiekio mažinimas yra neatsiejamas ir nuo pritaikytos ir standartizuotosios duomenų apsaugos principo. Pritaikytos ir standartizuotosios apsaugos principas reikalauja, jog kiekvienas duomenų valdytojas, renkant duomenis, turi tiksliai apibrėžti, kokie asmens duomenys iš tikrųjų reikalingi. Turėtų būti taikomi konkretūs procesai, kad nereikalingi asmens duomenys būtų pašalinti iš rinkimo ir (ar) perdavimo. Pavyzdžiui, turi būti numatomi automatizuoti trynimo mechanizmai (D' Acquisto *et al*., 2015, p. 22).

Taip pat svarbu paminėti, jog duomenų kiekio mažinimas skatina duomenų nuasmeninimo praktiką (Zaleskis, 2019, p. 123). Duomenų apsaugos principai neturėtų būti taikomi anoniminei informacijai, t.y. tokiai, kuri yra nesusijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali būti nustatyta, pavyzdžiui, duomenis tvarkant statistikos tikslais (BDAR preambulės 26 punktas, cituota Zaleskis, 2019, p. 123). Organizacijos, naudojančios anoniminius duomenis, turi sugebėti įrodyti, kad atliko

pakartotinio identifikavimo rizikos vertinimą ir priėmė rizikai proporcingus sprendimus (Information Commissioner‘s Office, 2014, p. 13).

Atsižvelgiant į duomenų kiekio mažinimo ir su juo susijusių principų pažeidimus praktikoje, 2018 m. Danijos duomenų apsaugos agentūra „Datatilsynet“ (toliau – Datatilsynet) didžiųjų duomenų bendrovei „Taxa 4×35” (toliau - Taxa) paskyrė baudą už duomenų saugojimo laikotarpių pažeidimą (Danish DPA Issues First Ever…, 2019). Taxa sistema renka įvairius duomenis, įskaitant kliento vardą, telefono numerį, kelionės datą, kelionės pradžios ir pabaigos laiką, nuvažiuotų kilometrų skaičių, mokėjimus, GPS kelionės pradžios ir pabaigos koordinates ir kt. duomenis. Taxa susieja šiuos duomenis su vartotojo mokesčių informacija, kad būtų užtikrinta tinkama mokesčių suma (Data anonymization and GDPR compliance…, 2019). Duomenų apsaugos agentūra nustatė, jog saugojimas prieštaravo duomenų kiekio mažinimo principui, įskaitant adekvatumo, tinkamumo ir apsiribojimo tuo, kas būtina duomenų tvarkymo tikslams (BDAR, 5 str.). Taip pat ir saugojimo trukmės apribojimo principui, reikalaujančiam, jog duomenys būtų saugomi forma, leidžiančia identifikuoti duomenų subjektus ne ilgiau, nei tai yra būtina tikslams, kuriais tvarkomi asmens duomenys (BDAR, 5 str.). Įmonė po dviejų metų išbraukė vardus, susijusius su kelionės įrašais (likę duomenys buvo ištrinti po penkerių metų), teigdama, jog taip buvo atliktas duomenų anonimizavimas. Datatilsynet išvadomis informaciją apie kliento apmokestinimą vis tiek galima priskirti telefono numeriu, kuris buvo išbrauktas tik po penkerių metų. Anonimizavimas nebuvo tinkamai įgyvendintas ir įmonė liko pažeidusia duomenų kiekio mažinimą bei kartu ir saugojimo trukmės apribojimo principą (Data anonymization and GDPR compliance…, 2019). Telefono numerį susieti su asmeniu yra paprasta, todėl vis tiek taikomas BDAR ir reikalaujama sumažinti duomenis, kurių saugojimo laikotarpiai jau pasibaigė (Data anonymization and GDPR compliance…, 2019). Šiame pavyzdyje išlaikyti duomenų bazę buvo verlo plėtra. Taxa galėjo nustatyti, kada ir kur jiems reikia vairuotojų, ir anonimizuoti duomenis, ištrinant visus kitus duomenis, išskyrus kelionės datą, kelionės pradžią ir pabaigos laiką, nuvažiuotų kilometrų skaičių bei kelionės pradžios ir pabaigos GPS koordinates. Taxa galėjo šiuos duomenis sugrupuoti pagal dieną ar vietą, o ne pagal paskyrą. Tokiu būdu įmonė galėtų nustatyti geografinius karštuosius taškus ir piko valandas vairuotojams, tačiau neleistų nustatyti atskirų duomenų subjektų (Data anonymization and GDPR compliance…, 2019).

Doktrinoje yra išsakomos nuomonės dėl didžiųjų duomenų sąveikos su duomenų kiekio mažinimu ir su juo susijusiais principais. Vienavertus, duomenų kiekio mažinimas, kaip

ir duomenų tikslo apribojimas gali pakenkti didžiųjų duomenų prigimčiai, kadangi ribojamas didžiųjų duomenų dydis ir naudojimas (Hildebrandt, 2013, cituota Zarsky, 2017, p. 1005). Neretai teigiama, jog galimas didžiųjų duomenų privalumas atrasti naujas tendencijas, koreliacijas, modelius ir santykius gali nepasireikšti. Manoma, jog tai gali būti reikšmingas didelių duomenų ekonominės ir socialinės naudos praradimas (Rubinstein, 2013, p. 75). Šiomis dienomis diskusija dėl didžiųjų duomenų daugiausia orientuota į ekonomiką. Svarbiausias klausimas yra ne tik rinkimas, saugojimas ir nuosavybė, bet ir tai, kaip didieji duomenys gali sukurti vertę, kokia yra jų ekonominė nauda ir kaip tai gali padėti pirmaujančioms įmonėms pralenkti savo konkurentus (Rubinstein, 2013, p. 76).

Tačiau, grįžtant prie galimybės duomenis anonimizuoti, kai tai techniškai įmanoma, kai duomenų valdytojas įvertino, jog duomenys negalėtų būti atkurti bei, kai įmonė gali naudoti analizę be asmens duomenų (Information Commissioner‘s Office, 2017, p. 58), anonimizavimas gali būti priemonė organizacijoms, padedanti atlikti novatorišką analizę ar saugojimą (Information Commissioner‘s Office, 2014, p. 24).

3.4. Duomenų tikslumo principas

BDAR 5 str. 1 d. d punktas nustato, jog duomenys turi būti a) tikslūs ir prireikus atnaujinami; b) turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi (BDAR, 5 str.). Taip pat šis principas nustatytas konvencijoje Nr. 108 ir EBPO gairėse. Tačiau, BDAR neapibrėžia, kokie duomenys laikomi tiksliais (Zaleskis, 2019, p. 124). Duomenų tikslumas apima asmens duomenų aktualumą laiko požiūriu. Renkami duomenys gali būti tikslūs, tačiau pasikeitus aplinkybėms, asmens duomenys gali tapti nebe aktualūs (Zaleskis, 2019, p. 124). Duomenų tikslumo principas gali būti pažeistas, jei duomenų valdytojas tvarko asmens duomenis žinodamas, kad duomenys yra pasenę (Zaleskis, 2019, p. 124). Be to, svarbu tai, jog teisiniame reguliavime nėra apibrėžtų priemonių sąrašo, kurių turėtų imtis valdytojai, siekdami įgyvendinti šį principą. Duomenų valdytojas, vadovaudamasis atsakomybės principu, pats turi nuspręsti, kokiomis priemonėmis jis gali pasiekti duomenų tikslumo principo įgyvendinimą (Zaleskis, 2019, p. 124).

Duomenų tikslumas yra susijęs su visais didžiųjų duomenų projekto etapais: rinkimu, analize ir taikymu (Information Commissioner‘s Office, 2017, p. 43). Paprastai tariant,

duomenų tikslumo principą valdytojas turi įgyvendinti visose duomenų tvarkymo operacijose (Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba, 2018, p. 127). Mašininis mokymasis turi būti prižiūrimas jau išankstinio apdorojimo etape, kad būtų užtikrinama įvesties duomenų kokybė (Information Commissioner‘s Office, 2017, p. 44). Įvesties duomenyse esant klaidų ir netikslumų, jų bus ir išvesties duomenyse (Information Commissioner‘s Office, 2017, p. 44). Duomenų tikslumo principas itin svarbus asmenų profiliavimo metu. Netikslūs įvesties duomenys gali sukelti neteisingas sveikatos, kreditingumo, draudimo rizikos ar kitas prognozes (Information Commissioner‘s Office, 2017, p. 45). Todėl, galima teigti, jog duomenų valdytojai turi dėti visas pastangas, kad būtų naudojami tikslūs duomenys, kadangi duomenų netikslumas gali tapti neteisingų ir neigiamą įtaką asmenims darančių prognozių priežastimi.

4. KITI ES BENDROJO DUOMENŲ APSAUGOS REGLAMENTO REIKALAVIMAI, TAIKOMI DIDŽIŲJŲ DUOMENŲ REGULIAVIMUI

4.1. Duomenų subjektų teisės

4.1.1. Teisė susipažinti su tvarkomais duomenimis

BDAR 15 str. 1 d. nustato, jog duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir informacija, kaip: a) tvarkymo tikslai; b) nustatytos atitinkamos asmens duomenų kategorijos; c) duomenų gavėjai ar duomenų gavėjų kategorijos, kuriems buvo ar bus atskleisti asmens duomenys, visų pirma duomenų gavėjai trečiosiose valstybėse ar tarptautinėse organizacijose; d) kai įmanoma, numatomas asmens duomenų saugojimo laikotarpis arba, jei neįmanoma, kriterijai, taikomi tam laikotarpiui nustatyti; e) teisė prašyti duomenų valdytojo ištaisyti ar ištrinti duomenis ar apriboti su duomenų subjektu susijusių duomenų tvarkymą arba nesutikti su tokiu tvarkymu; f) teisė pateikti skundą priežiūros institucijai, g) informacija apie šaltinius, kai duomenys renkami ne iš paties duomenų subjekto, h) informacija apie priimamą automatizuotą sprendimą, įskaitant profiliavimą ir jo logikos pagrindimą (BDAR, 15 str.). Be to, BDAR 15 str. 3 d. nustato, jog, kai duomenų subjektas prašymą pateikia elektroninėmis priemonėmis ir išskyrus atvejus, kai duomenų subjektas paprašo ją pateikti kitaip, informacija pateikiama įprastai naudojama elektronine forma (BDAR, 15 str.).

Duomenų subjekto teisė susipažinti su savo duomenimis ir atitinkama duomenų valdytojų pareiga supažindinti duomenų subjektus su jų duomenimis detalizuoja skaidrumo principą (Zaleskis, 2019, p. 171). Šios nuostatos atspindi duomenų subjekto galimybę susipažinti su apie jį surinktais asmens duomenimis, kad žinotų apie duomenų tvarkymą, galėtų patikrinti jo teisėtumą ir prireikus įgyvendinti kitas savo, kaip duomenų subjekto, teises (Zaleskis, 2019, p. 171).

BDAR 83 straipsnyje nurodyta, jog duomenų subjekto prieigos teisės pažeidimas gali užtraukti duomenų valdytojui nemažas baudas (iki 20 000 000 EUR arba iki 4% visos pasaulinės metinės apyvartos), todėl turėtų būti užtikrinta, kad tokie prašymai būtų tvarkomi ir vykdomi rūpestingai (Voigt, Von dem Bussche, 2017, p. 153). Pavyzdžiui, gali būti

naudojamos standartizuotos formos, kuriose yra visa svarbi informacija, nes norint atsakyti į duomenų subjekto prašymą, jo atitinkami asmens duomenys turės būti tik pridėti prie tokios formos (Walter, 2016, cituota Voigt, Von dem Bussche, 2017, p. 153).

Atsižvelgiant į šios teisės ir technologijų tarpusavio veikimo problematiką, teisė susipažinti su tvarkomais duomenimis kartais pasižymi sunkumais, su kuriais gali susidurti didžiųjų duomenų veikla užsiimančios organizacijos. Didžiųjų duomenų apimtis ir įvairovė gali apsunkinti organizacijų įsipareigojimų vykdymą (Information Commissioner‘s Office, 2017, p. 46). Pavyzdžiui, istoriškai bendra organizacijų problema dėl prašymų susipažinti su duomenimis buvo ta, kad informacija laikoma skirtingose vietose. Diskusijose su pramonės atstovais buvo pasiūlyta, kad jeigu organizacija pereina prie didžiųjų duomenų, atskiros duomenų saugyklos turi būti sujungtos, ir tai padeda lengviau surasti visus asmens duomenis (Information Commissioner‘s Office, 2017, p. 47). Be to, jeigu organizacija naudoja ir (arba) perka įvairius duomenų šaltinius, įskaitant nestruktūrizuotus duomenis, gali būti sunku pateikti visus duomenis apie vieną asmenį, kadangi informacija paprastai sudaro įvairių asmenų duomenų rinkinius (Information Commissioner‘s Office, 2017, p. 47). Tačiau, tokios priežastys negali būti teisinių įsipareigojimų nevykdymo pateisinimas (Information Commissioner‘s Office, 2017, p. 46). Taigi, nors kartais pareiga supažindinti asmenis su apie jais surinktais duomenimis gali būti ne itin paprasta užduotis, organizacijos, žinodamos, kokia veikla siekia užsiimti, privalo žinoti ir su šia veikla susijusias pareigas bei užtikrinti tinkamą ir teisėtą jos įgyvendinimą.

4.1.2. Teisė į duomenų perkeliamumą

Teisė į duomenų perkeliamumą yra viena iš svarbiausių BDAR naujovių (De Hert *et al*., 2018, p. 193). BDAR 20 str. nustato, jog duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir turi teisę persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių, kai: a) duomenų tvarkymas yra grindžiamas sutikimu ar sutartimi; b) duomenys yra tvarkomi automatizuotomis priemonėmis (BDAR, 20 str.). Tačiau, norint pasinaudoti teise į duomenų perkeliamumą, turi būti tenkinamos ir kitos BDAR nustatytos sąlygos:

1. Teisės į duomenų perkeliamumą pagrindu gaunama ir perkeliama informacija gali būti tik apie šia teise bandantį pasinaudoti duomenų subjektą (BDAR, 20 str.). Pavyzdžiui,

nuotraukos „Facebook", sudarančios kelis asmenis, vieno asmens prašymu negalėtų būti perkeliamos į kitą socialinių tinklų platformą (Engels, 2016, cituota Ishii, 2018, p. 340).

2. Teisė į duomenų perkeliamumą apima tik duomenis, kurie yra pateikti paties duomenų subjekto (BDAR, 20 str.). Duomenys pateikti duomenų subjekto laikomi dviejais atvejais. Pirma, subjektas pateikia aktyviai ir sąmoningai. Pavyzdžiui, elektroninio pašto adresus, vardą, amžių (Zaleskis, 2019, p. 176). Antra, tai gali būti stebėjimo duomenys, kuriuos duomenų subjektas pateikia naudodamasis tam tikra paslauga ar įrenginiu. Pavyzdžiui, atliktos paieškos istorija, vietos nustatymo ar neapdoroti išmaniųjų skaitiklių, aktyvumo ir sveikatos matuoklių duomenys (Zaleskis, 2019, p. 176). Svarbu tai, kad teisei į duomenų perkeliamumą nepriskiriami išvestiniai duomenys, kuriuos analizuodamas duomenis sugeneruoja duomenų valdytojas (Zaleskis, 2019, p. 176). Didžiųjų duomenų analizės kontekste šis „pateikiamų" duomenų apribojimas gali būti reikšminga duomenų valdytojų intelektinės nuosavybės apsauga, vengiant, kad skaitmeninių paslaugų teikėjo intelektinis darbas (duomenys apie vartotojus, gauti naudojant sudėtingus algoritmus) galėtų būti nemokamai atskleistas konkurencingoms įmonėms (Malgieri, 2016, cituota De Hert *et al.*, 2018, p. 199).

Be to, kaip ir minėta prieš tai, teisė į duomenų perkeliamumą gali būti įgyvendinama dviem būdais: a) asmuo gali gauti su savo asmens duomenis ir persiųsti juos kitam paslaugų teikėjui pats (BDAR, 20 str.); b) pasinaudoti teise, kad vienas duomenų valdytojas asmens duomenis tiesiogiai persiųstų kitam, kai tai techniškai įmanoma (BDAR, 20 str.). Teisė į duomenų perkeliamumą pasižymi „problemine galimybe" kalbant apie sistemų sąveikumą (De Hert *et al*., 2018, p. 200). BDAR preambulės 68 punktas nurodo, jog duomenų valdytojai „turėtų būti skatinami kurti sąveikius formatus, leidžiančius perkelti duomenis" (BDAR preambulės 68 punktas). Konstatuojamoji dalis nurodo, jog sistemos „turėtų būti skatinamos" ir neprivaloma kurti šių „sąveikių formatų" (De Hert *et al*., 2018, p. 201). Kitaip tariant, duomenų valdytojai gali užkirsti kelią visapusiškai naudotis teise į duomenų perkeliamumą, jeigu jie įrodo, kad tam tikroje situacijoje dėl jų organizacijos technologinio išsivystymo lygio techniškai neįmanoma perduoti duomenis kitam valdytojui (De Hert *et al*., 2018, p. 201).

Tačiau, nors ir duomenų perkėlimas iš vieno valdytojo kitam pasižymi ,,problemine galimybe“ (De Hert *et al*., 2018, p. 200), praktikoje jau yra tam tikrų sėkmingų pasiekimų, kuriuos įgyvendina didžiųjų duomenų bendrovės, kaip, pavyzdžiui:

1. ,,Data Transfer Project“ – Šis projektas praplėtė duomenų perkeliamumo teisę, suteikdamas vartotojams galimybę tiesiogiai perduoti duomenis bet kuriam projekte dalyvaujančiam tiekėjui ir iš jo. Projekte šiuo metu dalyvauja ,,Google“, ,,Microsoft“, ,,Apple“, Facebook“ ir ,,Twitter“ (Data Transfer Project, 2018).
2. ,,Telegram“ - populiari daugiašalė susirašinėjimo programa, kuri yra plačiai naudojama, kadangi siūlo keletą patobulintų privatumo ir šifravimo funkcijų. Programa prisijungė daugiau nei 100 milijonų naujų vartotojų, siekiančių daugiau privatumo ir laisvės. Atsižvelgiant į duomenų perkeliamumo galimybes, ,,Telegram“ kiekvienam vartotojui suteikia teisę perkelti savo pokalbių istoriją, įskaitant vaizdo įrašus ir dokumentus, į ,,Telegram“, iš tokių programų, kaip ,,WhatsApp“, ,,Line“ ar kt. (Moving Chat History from Other..., 2021).

Taigi, nors teisė į duomenų perkeliamumą pasižymi autorių įvardijamomis problemomis dėl sistemų saveikumo, kuomet norima perkelti duomenis iš vieno valdytojo kitam, praktikoje galima atrasti pavyzdžių, kuomet šią teisę visapusiškai įgyvendina kai kurios didžiųjų duomenų organizacijos, taip pat ir skaitmeniniai gigantai.

4.1.3. Teisė reikalauti ištrinti duomenis („Teisė būti pamirštam“)

BDAR ,,teisė būti pamirštam'' įtvirtinta 17 straipsnyje. Šio straipsnio 1 d. nustato, jog tam tikrais atvejais duomenų subjektas turi teisę reikalauti, jog duomenų valdytojas nedelsdamas ištrintų su juo susijusius duomenis, o duomenų valdytojas yra įpareigotas tai padaryti (BDAR, 17 str.). Remiantis to paties straipsnio 1 dalimi, teisė reikalauti, kad asmens duomenys būtų ištrinti galima, kai: a) asmens duomenys nebėra būtini tikslams, kuriems jie buvo surinkti b) duomenų subjektas atšaukia sutikimą, kuriuo grindžiamas tvarkymas, ir nėra jokio kito teisinio pagrindo tvarkyti duomenis; c) duomenų subjektas įgyvendina savo teisę nesutikti su jo duomenų tvarkymu, d) duomenys buvo tvarkomi neteisėtai, e) duomenys turi būti ištrinti pagal nustatytą teisinę prievolę; f) duomenys buvo surinkti visuomenės paslaugų siūlymo kontekste (BDAR, 17 str.). Didžiųjų duomenų kontekste didelę reikšmę turi BDAR 17 str. 2 dalis. Ši dalis nustato, kad, kai duomenų valdytojas viešai paskelbė asmens duomenis ir pagal 1 dalį

privalo asmens duomenis ištrinti, duomenų valdytojas, atsižvelgdamas į turimas technologijas ir įgyvendinimo sąnaudas, imasi pagrįstų veiksmų, įskaitant technines priemones, kad informuotų duomenis tvarkančius duomenų valdytojus, jog duomenų subjektas paprašė, kad tokie duomenų valdytojai ištrintų visas nuorodas į tuos asmens duomenis arba jų kopijas ar dublikatus (BDAR, 17 str.). Taip pat, ši teisė yra subjektyvi, todėl duomenų subjektas turi įrodyti, kad egzistuoja jo teisė ištrinti duomenis, t.y. turi būti įpareigotas nurodyti vieną iš 17 str. 1 dalies sąlygų (Voigt, Von dem Bussche, 2017, p. 154).

Be to, ši teisė nėra absoliuti. BDAR 17 str. 3 dalyje yra nurodytos išimtys. Teisė gali būti netaikoma: a) siekiant pasinaudoti teise į saviraiškos ir informacijos laisvę; b) siekiant laikytis teisinės prievolės, kuria reikalaujama tvarkyti duomenis, arba siekiant atlikti užduotį, vykdomą viešojo intereso labui, arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas; c) dėl viešojo intereso priežasčių visuomenės sveikatos srityje, d) archyvavimo, mokslinių ar istorinių tyrimų, statistikos tikslais; e) pareiškiant, vykdant ar apginant teisinius reikalavimus (BDAR, 17 str.). Atsižvelgiant į išimtis, paieškos rezultatų nuorodų panaikinimas gali neigiamai paveikti kitus, kaip, pavyzdžiui, interneto vartotojus, bandančius gauti informacijos apie buvusį įvykį. Todėl, kiekvieju konkrečiu atveju ir remiantis BDAR nuostatomis, leidžiančiomis atsisakyti įvydyti tokį prašymą, reikalingas konkretus vertinimas tarp pateikusio prašymą asmens interesų ir galimybės neleisti pasinaudoti šia teise (Globocnik, 2020, p. 381).

Be to, svarbu prisiminti, jog internetinės pretenzijos dėl „teisės būti pamirštam" duomenų apsaugos srityje išpopuliarėjo, kai Europos Komisija nusprendė įtraukti šį frazeologizmą į BDAR nuostatas (Erdos, Garstka, 2019, p. 1). Naujos formuluotės atsiradimą paskatino platus duomenų skelbimas internete. Taip pat aiškaus „teisės būti pamirštam" pripažinimo rezultatą simbolizavo socialinių tinklų populiarėjimas (Erdos, Garstka, 2019, p. 1). Buvusioje Duomenų apsaugos direktyvoje jau buvo įtvirtinti principai, pagrindžiantys teisę būti pamirštam, tačiau BDAR jie buvo dar kartą patvirtinami ir pertvarkomi, kad geriau atitiktų šiuolaikinę informacinę visuomenę (Custers, Uršič, 2016, p. 10). Be to, pastarąją teisę išplėsti BDAR paskatino ir *Google Spain* sprendimas, kurio pagrindu buvo pripažinta, jog asmenys turi kvalifikuotą teisę būti „užmiršti" pagal rezultatus, gautus atlikus bet kokią interneto paiešką pagal asmenvardį (*Google Spain ir Google*, 2014, 94 punktas). ESTT išaiškino, kad teisė būti pamirštam interneto paieškos rezultatuose iš esmės yra viršesnė už visuomenės interesą turėti prieigą prie šios informacijos (Zaleskis, 2019, p. 186).

Teisė būti pamirštam neatsiejama nuo šių dienų kasdieninio interneto naudojimo. Didžiųjų duomenų įmonės, tokios kaip „Facebook“, „Google“, „Youtube“ ar kt. naudoja specialias formas, galinčias asmenis pareikalauti ištrinti tam tikrus „URL“ iš paieškos sistemų. Faktinis pašalintų „URL“ skaičius nuo 2014 m., kuriais buvo priimtas *Google Spain* sprendimas, išaugo nuo 500 tūkst. iki 4 mln. (Google Transparency Report, 2021).

Be to, svarbu paminėti, ką apie „teisę būti pamirštam“ diskutuoja technologijų specialistų bendruomenė. Atsižvelgiant į 17 str. nuostatų ir technologijų tarpusavio ryšį, ginčijamas „pamiršimo” sąvokų suvokimas interneto tinklalapiuose. Norint suprasti teisę būti pamirštam didžiųjų duomenų analizės kontekste, pirmiausia reikia įsigilinti į žmogaus ir dirbtinio atminimo bei pamiršimo sąvokų apžvalgą (Villaronga *et al*., 2018, p. 7). Panašu, kad dabartinis įstatymas traktuoja vienodai žmogaus ir mašinos atmintį, t.y. palaiko fiktyvų atminties supratimą (Villaronga *et al*., 2018, p. 7). Teisė būti pamirštam iš esmės taiko žmogaus atminties metaforą dėl informacijos “pamiršimo”. Asmenims prašant ištrinti jų asmeninę informaciją yra tolygu metaforiškai reikalauti, kad kiti tai pamirštų. Tačiau, ši metafora būdinga tik žmogaus protams ir nėra vertinama kaip dirbtinio intelekto ar mašininio mokymosi era (Villaronga *et al*., 2018, p. 7). Dirbtinis intelektas „nepamiršta” duomenų taip, kaip tai daro žmonės. Teigiama, jog dabartinėse sistemose duomenų pašalinimas yra labai sudėtingas. Interneto tinklalapiuose duomenys teisės būti pamirštam kontekste ištrinami tik iš paieškos indeksų (Villaronga *et al*., 2018, p. 8). Duomenų valdytojo užduotis nėra ištrinti pačią informaciją, o tik nuorodą, susijusią su ja bei informaciją vis tiek galima rasti žiniatinklyje, tik kitomis tyrimo priemonėmis. Visiškas ištrynimas iš duomenų bazių būtų milžiniškos papildomos pastangos, darančios rimtą poveikį bei kartais galėtų reikšti, kad prašymas ištrinti būtų brangesnis nei keli duomenų įterpimai (Villaronga *et al*., 2018, p. 8).

Taigi didžiųjų duomenų sistemų kontekste ir BDAR reikalavime pasižymi „pamiršimo” sąvokų skirtumas. Diskusijos dėl teisės būti pamirštam reikšmės analizuojant duomenis praktikoje paliestos mažai, tačiau paprastai teigiama, jog didžiųjų duomenų analizės sistemose informacija išlieka. Tačiau, ši teisė, kuomet prašoma ištrinti duomenis iš puslapių nuorodų, nors ir nepanaikina informacijos iš duomenų sistemų, gali būti naudinga asmenims tuo požiūriu, jog tam tikra juos siejanti informacija nebūtų akivaizdžiai prieinama kitiems asmenims bent jau puslapių nuorodose, kurias asmenys prašo pašalinti.

4.1.4. Automatizuotas atskirų sprendimų priėmimas

4.1.4.1. Teisė netaikyti automatizuoto sprendimo

BDAR 22 str. 1 d. nustato, jog duomenų subjektas turi teisę, 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 (BDAR, 22 str.). Šis straipsnis aiškiai mini profiliavimą kaip vieną taikymo sritį, nes ši apdorojimo veikla tampa vis aktualesnė praktikoje. BDAR 4 str. 4 punktas nurodo, jog profiliavimą sudaro bet kokios formos automatizuotas asmens duomenų tvarkymas, vertinant asmens aspektus susijusius su asmeniu, visų pirma siekiant analizuoti ar numatyti aspektus, susijusius su duomenų subjekto darbe, ekonomine situacija, sveikata, asmeninėmis nuostomis ar interesais, patikimumu ar elgesiu, vieta ar judėjimu (BDAR, 4 str.).

BDAR 22 str. 1 dalies teise galima pasinaudoti tik esant BDAR nustatytomis sąlygomis. Pirma, gali būti netaikomas taikomas "tik" automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas (ES 29 str. Darbo grupė, 2017, p. 9). Pavyzdžiui, pagal tam tikrą algoritmą priimamas sprendimas, ar suteikti paskolą, ir tas sprendimas automatiškai pateikiamas asmeniui, jokiam žmogui prieš tai neatlikus jokio prasmingo vertinimo (ES 29 str. Darbo grupė, 2017, p. 9). Svarbu tai, kad duomenų valdytojas negali imituoti žmogaus įsikišimo ir taip išvengti 22 straipsnio nuostatų. Pavyzdžiui, jei žmogus nuolat asmenims taiko automatiškai sudarytus profilius ir tai neturi jokio faktinio poveikio rezultatui, vis vien bus laikoma, kad sprendimas grindžiamas tik automatizuotu duomenų tvarkymu (ES 29 str. Darbo grupė, 2017, p. 22).

Antra, asmeniui turi kilti teisinės pasekmės ar kitu panašiu būdu turi būti daromas didelis poveikis (BDAR, 22str.). Pavyzdžiui, teisinės pasekmės galėtų būti sutarties nutraukimas ar socialinės išmokos vaikui išlaikyti neišdavimas (ES 29 str. Darbo grupė, 2017, p. 22). Be to, jeigu nepasikeičia duomenų subjekto juridinės teisės arba pareigos, jam vis tiek gali būti padarytas pakankamai didelis poveikis, kad pagal 22 str. reikėtų taikyti apsaugos priemones (ES 29 str. Darbo grupė, 2017, p. 23). Pavyzdžiui, sprendimai, kurie turi poveikio asmens finansinėms aplinkybėms, kaip galimybei gauti kreditą ar galimybei gauti sveikatos priežiūros paslaugas (ES 29 str. Darbo grupė, 2017, p. 23).

Be to, teisė netaikyti automatizuoto sprendimo, įskaitant profiavimą, kaip ir dauguma kitų reglamento teisių, turi tam tikras išimtis. Draudimas netaikomas, jei automatizuotas sprendimų priėmimas: a) pagrįstas aiškiu asmens sutikimu; b) yra leidžiamas Sąjungos arba valstybės narės teisėje, kurie taikomi duomenų valdytojui ir kuriais taip pat nustatomos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti; c) yra būtinas asmens ir valdytojo sutarčiai sudaryti (BDAR, 22 str.). Pavyzdžiui, bankas norėtų sudaryti paskolos sutartį su duomenų subjektu ir remdamasis didžiųjų duomenų analize priimtų atitinkamą sprendimą, susijusį su pareiškėjo elgsena (Zuiderveen Borgesius, 2018, p. 8).

Taip pat yra užtikrinama garantija jei duomenų valdytojas norėtų apeiti tokį draudimą, kuomet pasikliaujama sutarties ar sutikimo išimtimi. BDAR 22 str. 3 dalis nurodo, jog duomenų valdytojas įgyvendina tinkamas priemones duomenų subjekto teisėms ir laisvėms bei teisėtiems ineteresams apsaugoti ir duomenų subjektas turi teisę pareikalauti žmogaus įsikišimo, pareikšti savo požiūrį ir užginčyti sprendimą (BDAR, 22 str.). Pavyzdžiui, bankas galėtų užtikrinti, jog klientai galėtų paskambinti į banką su prašymu pareikalaujant kompetentingo darbuotojo dar kartą peržiūrėti automatizuotą sprendimą, jei bankas automatiškai atsisako suteikti paskolą per banko svetainę (Zuiderveen Borgesius, 2018, p. 23).

Be to, BDAR 22 str. yra tiesiogiai susijęs su BDAR 13-15 str. prievolėmis. Svarbu, jog norėdamas pasinaudoti teise netaikyti automatizuoto sprendimo, duomenų subjektas pirmiausia turi žinoti, ar sprendimas jam apskritai yra taikomas (Selbst, Powles, 2017, p. 234). BDAR 13 str. 2 dalies f punktas, 14 str. 2 dalies g punktas ir 15 str. 1 dalies h punktas reikalauja, kad duomenų valdytojai teiktų duomenų subjektams informaciją apie automatizuotų sprendimų, įskaitant profiliavimą, buvimą bei 22 str. 1 ir 4 dalyse nurodytą informaciją, ir bent jau tokiais atvejais prasmingą informaciją apie logiką, taip pat apie tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (Selbst, Powles, 2017, p. 234). Atsižvelgiant į logiką, duomenų valdytojas turėtų pateikti duomenų subjektui bendrą informaciją (pirmiausia – apie veiksnius, į kuriuos atsižvelgta priimant sprendimą, ir atitinkamą kiekvieno iš jų įtaką bendram rezultatui), kuri jam taip pat būtų naudinga norint užginčyti sprendimą (ES 29 str. Darbo grupė, 2017, p. 29).

Didžiųjų duomenų kontekste automatizuotas sprendimų priėmimas vertinamas kaip procesas, kurio metu vis didėjantis duomenų kiekis ir įvairovė apdorojami algoritmais, kurie vėliau naudojami priimant duomenimis pagrįstus sprendimus (Newell, Marabelli, 2015 cituota

Araujo *et al*., 2020, p. 612). Plačiąja prasme algoritmai yra užkoduotos procedūros, kuomet įvesties duomenys transformuojami į norimą išvestį (Gillespie, 2014, cituota Castets – Renard, 2019, p. 97). Ši procedūra apima dirbtinio intelekto apdorojimą, kuris apima mašininį mokymąsi ir giluminį mokymąsi (Surden, 2014, cituota Castets - Renard, 2019, p. 97). Mašininis mokymasis turėtų suteikti kompiuterinei sistemai galimybę laipsniškai gerinti konkrečios užduoties atlikimą, remiantis duomenų gavyba ir masiniu duomenų rinkimu (Veale ,Binns, 2017, cituota Castets - Renard, 2019, p. 98). Mašininio mokymosi, algoritmų išradimo ir jų konfigūravimo galimybėmis gaunami sprendimai akivaizdžiai naudingi finansinėje, bankininkysės, draudimo, visuomenės sveikatos ir daugelio kitų paslaugų atžvilgiu (Brkan, 2019, p. 92). Tačiau, dėl algoritminio sprendimų priėmimo, naudojant vien tik automatizuotas priemones, gali būti priimami diskriminuojantys ar nesąžiningi sprendimai. Todėl, galima teigti, jog BDAR 22 str. 1 dalis yra gerosios valios pavyzdys bei vienas iš siekių skirtų sumažinti tokių sprendimų keliamai rizikai, leidžiant asmenims pasinaudoti teise netaikyti visiškai automatizuotomis priemonėmis priimto sprendimo.

4.1.4.2. Automatizuotas sprendimų priėmimas ir diskriminacija

BDAR 22 str. neužkerta kelio taikyti automatizuotomis priemonėmis priimtus sprendimus, nors ir suteikia asmenims kvalifikuotą teisę nebūti tokių sprendimų subjektais (Information Commissioner‘s Office, 2017, p. 21). Remiantis BDAR 22 str. 2 dalimi, tais atvejais, kai sutartis ar sutikimas yra profiliavimo pagrindas, turėtų būti įgyvendinamos tinkamos priemonės duomenų subjekto teisėms ir laisvėms apsaugoti (BDAR, 22 str.). Priimant automatizuotą sprendimą svarbu atsižvelgti ir į tai, kad toks sprendimas gali būti diskriminuojantis. Diskriminacija bendrai yra apibrėžiama kaip nesąžiningas elgesys su asmeniu dėl jo narystės tam tikroje grupėje, rasės, lyties ar kt. (Altman, 2015, cituota Goodman, Flaxman, 2017, p. 53). Profiliavimas atliekamas, kai duomenų subjektai yra grupuojami pagal įvairius kintamuosius, o sprendimai priimami remiantis subjektų priklausymu tam tikromis apibrėžtomis grupėmis, todėl, nenuostabu, kad susirūpinimas diskriminacija pradėjo vyrauti diskusijose dėl didžiųjų duomenų etikos (Goodman, Flaxman, 2017, p. 53).

BDAR 22 str. tiesiogiai nenurodo diskriminacijos draudimo, tačiau tokia nuostata kyla iš BDAR preambulės 71 punkto, kuriame nurodyta, jog norint, kad būtų užtikrintas sąžiningas ir skaidrus asmens duomenų tvarkymas, duomenų valdytojas profiliavimui turėtų naudoti tinkamas matematines ar statistines procedūras, įgyvendinti technines ir organizacines priemones, tinkamas apsisaugoti nuo diskriminacinio poveikio fiziniams asmenims dėl rasės ar etninės kilmės, politinių pažiūrų, religijos ar kt. (BDAR preambulės 71 punktas). Be to, galima paminėti, jog diskriminacijos draudimas kyla ir iš ES Chartijos 21 str., pagal kurį draudžiama bet kokia diskriminacija dėl asmens lyties, rasės, odos spalvos, tautinės ar socialinės kilmės, genetinių bruožų, kalbos, religijos ar tikėjimo, politinių ar kitokių pažiūrų, priklausymo tautinei mažumai, turtinės padėties, gimimo, negalios, amžiaus, seksualinės orientacijos (Europos Sąjungos pagrindinių teisių chartija, 2012). BDAR 22 straipsnyje nurodyta, jog 2 dalies a ir c punktų atvejais, kuomet taikomas automatizuotas sprendimas, turi būti apsaugotos asmenų teisės ir laisvės (BDAR 22 str.), o pati ES Chartija iš savęs pagrindinių teisių apsaugą laiko kaip pagrindinį tikslą (Europos Sąjungos pagrindinių teisių chartija, 2012). Todėl, nors ir 22 str. tiesiogiai nenurodo diskriminavimo draudimo, atsižvelgiant į patį BDAR konstatuojamosios dalies tekstą ir kitus susijusius šaltinius akivaizdu, jog automatizuotas sprendimų priėmimas turi būti vykdomas siekiant išvengti galimų diskriminuojančių rezultatų.

Europos įstatymai nagrinėja dvi bendras diskriminacijos rūšis: tiesioginę ir netiesioginę (Watson, Ellis, cituota Wachter *et al.,* 2020, p. 15). Tiesioginė diskriminacija reiškia neigiamą elgesį, pagrįstą saugumo požymiu, pavyzdžiui, seksualine orientacija ar lytimi (Wachter, *et al.,* 2020, p. 15). Tiesiogiai diskriminuojančio automatizuoto sprendimo pavyzdys galėtų būti darbo nesuteikimas dėl rasės, pavyzdžiui, buvimo juodaodžiu. Netiesioginė diskriminacija apibūdina situaciją, kai akivaizdžiai „neutrali nuostata, kriterijus ar praktika“ neproporcingai ir nepalankiai veikia saugomą grupę, lyginant su kitais žmonėmis (*Debra Allonby prieš Accrington & Rossendale College* sprendimas, 2004, cituota Wachter *et al.,* 2020, p. 17). Pavyzdžiui, remdamasis geografiniu pranašumu bankas galėtų nuspręsti nesiūlyti hipotekų pagal vietovės kodus (pašto kodus) arba siūlyti jas tik esant mažiau palankioms sąlygoms. Ši taisyklė nėra pagrįsta specialiųjų kategorijų duomenimis. Tačiau, jei tokiose vietovėse yra rasiniu būdu atskirti rajonai (Schelling, 1997, cituota Rhoen, Yi Feng, 2018, p. 150), toks sprendimų priėmimo procesas gali būti netiesioginės diskriminacijos dėl jautrios savybės pavyzdys. Panašūs pavyzdžiai galėtų būti užimtumo, švietimo, sveikatos apsaugos ar kt. srityse (Rhoen, Yi Feng, 2018, p. 150).

ES 29 str. Darbo grupė, remdamasi 22 str. ir BDAR preambulės 71 punkto nuostatomis išskiria galimas priemones, siekiant išvengti diskriminacijos. Duomenų valdytojams pateikiamas nebaigtinis rekomenduojamos gerosios praktikos pavyzdžių sąrašas, į kurį duomenų valdytojai galėtų atsižvelgti taikydami visiškai automatizuotą sprendimų priėmimą, įskaitant profiliavimą, ir tai gali būti reguliarios savo sistemų kokybės užtikrinimo patikros, kuriomis siekiama užtikrinti, kad su asmenimis būtų elgiamasi sąžiningai ir kad jie nebūtų diskriminuojami remiantis specialiųjų kategorijų asmens duomenimis (ES 29 str. Darbo grupė, 2017, p. 34); algoritmų patikros, kaip naudojamų algoritmų, kuriuos parengė mašinų mokymosi sistemos, tikrinimas siekiant įrodyti, kad jie iš tikrųjų veikia taip, kaip numatyta, ir kad juos taikant negaunama diskriminuojamojo pobūdžio, klaidingų arba nepagrįstų rezultatų (ES 29 str. Darbo grupė, 2017, p. 35). Visų tipų algoritmams auditas yra būtina sąlyga norint patikrinti, ar algoritmai veikia tinkamai (Mittelstadt, 2016, p. 4994). Trečiajai šaliai atliekant nepriklausomą auditą (kai profiliavimu grindžiamas sprendimų priėmimas daro didelį poveikį asmenims), auditoriui pateikiama visa reikiama informacija apie tai, kaip veikia algoritmas arba mašininio mokymosi sistema (ES 29 str. Darbo grupė, 2017, p. 35). Paprastai tariant, audito metodai gali būti naudojami norint nustatyti veiksnius, kurie daro įtaką algoritminiam sprendimui (Information Commissioner‘s Office, 2017, p. 86). Pripažįstama, jog algoritminiai auditai yra būtini nustatyti diskriminacinį poveikį, tačiau bet kada gali atsirasti naujų savybių, o algoritmai nuolat bus tobulinami, tad manoma, jog auditų reikšmingumas gali būti naudingas tik ribotą laiką (Rhoen, Yi Feng, 2018, p. 157). Sistemų algoritmai geba suskirstyti populiacijas ir rezultatus pagal duomenis ir ypatybes, klasifikavimo taisykles, kurias jie patys pateikia ir kuria bei numanomus duomenų ir sistemos projektavimo šališkumus (Friedman, Nissenbaum, 1996, cituota Wachter, 2020, p. 11), todėl gali pasitaikyti atvejų, kuomet netiesioginės diskriminacijos formos galėtų būti ir neaptinkamos.

Taigi galima daryti išvadą, kad norint išvengti diskriminuojančių ir nesąžiningų sprendimų algoritmai turi būti audituojami, tačiau, žvelgiant į nuolatinį technologijos buvimą priekyje ją kontroliuojančių metodų, algoritmai gali atrasti naujas diskriminavimo formas, kurioms ne visuomet gali būti pasiruošę algoritminiai auditai.

4.2. Poveikio duomenų apsaugai vertinimas

Poveikio duomenų apsaugai vertinimas yra vienas iš naujų BDAR reikalavimų. BDAR šį vertinimą įvedė kaip reikalavimą, atspindintį pritaikytosios duomenų apsaugos principą (Kaminski, Malgieri, 2020, p. 19), reikalaujantį rasti kūrybiškus techninius sprendimus, galinčius suteikti projektams pranašumų bei sumažinti privatumo riziką (Information Commissioner‘s Office, 2017, p. 72).

BDAR 35 str. 1 d. nustato, jog tais atvejais, kai dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą (BDAR, 35 str.). BDAR 3 d. nustato, jog remiantis 1 dalyje nurodytu poreikiu, toks vertinimas atliekamas, kai vykdomas: a) automatizuotas sprendimų priėmimas, įskaitant profiliavimą pagal BDAR 22 straipsnį; b) specialių kategorijų duomenų arba apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu; arba c) sistemingas viešos vietos stebėjimas dideliu mastu (BDAR, 35 str.). Atsižvelgiant į 35 str. 3 d. pirmąjį atvejį, ES 29 straipsnio darbo grupė pažymi, jog šio atvejo kontekste kalbama apie automatizuotus sprendimus, įskaitant profiliavimą, kurie yra grindžiami „tik“ automatizuotu duomenų tvarkymu, taip pat ir ne visiškai automatizuotu duomenų tvarkymu (ES 29 str. Darbo grupė, 2017, p. 32). Tai reiškia, jog 35 straipsnio 3 dalies a punktas bus taikomas tuo atveju, kai sprendimų priėmimas, įskaitant profiliavimą, dėl kurio kyla teisinių pasekmių arba panašiu būdu daromas didelis poveikis nėra visiškai automatizuotas, o taip pat, kai sprendimų priėmimas yra visiškai automatizuotas, kaip apibrėžta BDAR 22 straipsnio 1 dalyje (ES 29 str. Darbo grupė, 2017, p. 32).

Didžiųjų duomenų analizės vykdymas gali būti nukreiptas ne tik į materialų algoritmų poveikį, duomenų valdytojų laikymąsi duomenų apsaugos principų, tačiau ir į kitus reikalavimus, kaip, pavyzdžiui, poveikio duomenų apsaugai vertinimo poreikį (Rhoen, Yi Feng, 2018, p. 157). Didžiųjų duomenų kontekste poveikio duomenų apsaugai vertinimas svarbus, nes didžiųjų duomenų veiklą paprastai sudaro sistemingas ir išsamus asmens duomenų analizavimas, o poveikio duomenų apsaugai vertinimas gali padėti nustatyti numatomos tvarkymo veiklos pobūdį ir riziką (Voigt, Von dem Bussche, 2017, p. 238). Be to, akivaizdu, jog 35 str. 3 d. a punkto aiškinimas, pažymintis automatizuotą sprendimų priėmimą,

įskaitant profiliavimą, galėtų nulemti, kad šie vertinimai beveik visada reikalingi didžiųjų duomenų rinkiniams (Rhoen, Yi Feng, 2018, p. 157).

BDAR 35 str. 7 dalyje nurodyti keturi poveikio duomenų apsaugai etapai (BDAR, 35 str.). Poveikio duomenų apsaugai vertinimas atliekamas kiekvienu individualiu atveju skirtingai. Taip pat lemtingą įtaką gali turėti ir valstybių narių nacionalinė praktika, tačiau atsižvelgiant į 7 dalies nuostatas, išskiriamos atitinkamos rekomendacijos, kuriomis galėtų vadovautis duomenų valdytojai, kurie ketina užsiimti naujų technologijų veikla (Information Commissioner‘s Office, 2017, p. 99).

Pirma, vertinime sistemingai aprašomi tikslai ir priemonės, kuriais šie tikslai turėtų būti įgyvendinti (BDAR, 35 str.). Tikslų nustatymas yra svarbus kiekvienu konkrečiu ketinimu, tačiau, vėlgi, grįžtant prie didžiųjų duomenų bruožo atrasti netikėtas duomenų panaudojimo galimybės, vienas iš sprendimų galėtų būti už duomenų apsaugos teisės ribų. Pavyzdžiui, didelių duomenų projektams, kurių pradžioje nėra jokių tikslų ar uždavinių, atradimo etape naudoti tik anoniminius duomenis, ir tuo atveju, jei būtų aptikta naujų interesų sąsajų, organizacija galėtų nustatyti tolesnio apdorojimo tikslus prieš pradėdama bet kokio pirminio duomenų rinkinio, kuriame yra asmens duomenys, analizę (Information Commissioner‘s Office, 2017, p. 104).

Antra, atliekamas duomenų tvarkymo būtinumo ir proporcingumo vertinimas, susijęs su nustatytais tikslais (BDAR, 35 str.). Vertinant proporcingumą reikia apsvarstyti, ar projekto tikslai yra tiek svarbūs, kad pateisintų galimus naudoti privatumą pažeidžiančius metodus (Information Commissioner‘s Office, 2017, p. 106).

Trečia, atliekamas rizikos duomenų subjektų teisėms ir laisvėms vertinimas (BDAR, 35 str.) Organizacijos turi parengti savo klausimus rizikai nustatyti, remdamosios didžiųjų duomenų analizės, kurią jos atlieka, ypatumais (Information Commissioner‘s Office, 2017, p. 105). Pavyzdžiui, ar novatoriški metodai nekelia pavojaus sukelti neskaidrumo problemas, sukuriant ,,juodosios dėžės“ efektą. Taip pat, pavyzdžiui, ar analizė galėtų apimti specialiųjų kategorijų asmens duomenis analizuojant socialinės žiniasklaidos pranešimus (Information Commissioner‘s Office, 2017, p. 105)

Galiausiai, numatomos priemonės rizikai pašalinti, įskaitant saugumą, apsaugos priemones ir mechanizmus, užtikrinančius asmens duomenų apsaugą (BDAR, 35 str.). Pavyzdžiui, jei kyla ,,juodosios dėžės efekto” tikimybė, problemai spręsti galėtų būti taikomos

priemonės, užtikrinančios, kad algoritmai audituojami (Information Commissioner‘s Office, 2017, p. 109).

Be to, atsižvelgiant į konsultacijas su duomenų subjektais, BDAR nurodoma, jog su duomenų subjektais reikės konsultuotis, kai tai bus „tinkama“. BDAR tokių aplinkybių neapibrėžia, tačiau reikalavimas greičiausiai bus taikomas situacijose, kai duomenų subjektai bus reikšmingai paveikti didžiųjų duomenų analizės rezultatų (Information Commissioner‘s Office, 2017, p. 107). Tačiau, nors ir piliečių dalyvavimas viena vertus galėtų būti prasmingas, neretai teigiama, jog tik visuomenės dalyvavimas turėtų būti vertinamas kaip nepakankama priežiūra (Kaminski, Malgieri, 2020, p. 15). Manoma, jog prieš didžiųjų duomenų analizės naudojimą turėtų būti remiamasi ne tik apklausų informacija, tačiau ir atstovaujamųjų tarybų pagalba. Taip pat teigiama, kad dalyvauti turėtų ne tik išorės techniniai ekspertai, bet ir teisės, ir etikos ekspertai, kurie padėtų apibrėžti, ar aptarti diskusijas apie tai, ką turima omenyje, kaip „diskriminaciją“ ar „šališkumą“ (Kaminski, Malgieri, 2020, p. 15).

Taigi, remiantis šių aspektų visuma, galima teigti, jog poveikio duomenų apsaugai vertinimas yra vienas iš svarbių BDAR reikalavimų, kurio atlikimo metu galima identifikuoti didžiųjų duomenų analizės būsimus iššūkius bei nustatyti jų sprendimo variantus.

IŠVADOS

1. Didžiųjų duomenų, apimančių asmens duomenis, analizavimas, saugojimas, apdorojimas ar bet koks kitas tokių duomenų tvarkymas kelia grėsmę asmenims bei jų privatumui, esančiam vienu svarbiausių duomenų apsaugos teisės tikslų. Todėl, siekiant užtikrinti asmens duomenų, sudarančių didžiųjų duomenų rinkinius, apsaugą, reikalaujama laikytis duomenų apsaugos teisės nustatytų taisyklių.
2. Didieji duomenys dėl savo pobūdžio kelti grėsmę asmenims ir jų privatumui yra reguliuojami bendraisiais tarptautinės ir ES duomenų apsaugos teisės šaltiniais. Pagrindinis bendrasis ES duomenų apsaugos teisės šaltinis yra BDAR. Neskaitant bendrųjų duomenų apsaugos šaltinių, tarptautinėje teisėje yra priimtos Europos Tarybos gairės, skirtos specifiškai didiesiems duomenims ir jų analizei, kurios pripažįstamos suderintomis su BDAR nuostatomis, todėl valstybės narės gali jomis remtis nepažeidžiant ES nustatytų duomenų apsaugos teisės įsipareigojimų.
3. Visų BDAR nustatytų taisyklių laikymasis pirmiausia yra privalomas didžiųjų duomenų organizacijoms ar analizės įmonėms įsisteigusioms ES šalyse. Taip pat BDAR reguliavimas yra privalomas ir ES šalyse neįsisteigusioms didžiųjų duomenų organizacijoms, kurios siūlo prekes ar paslaugas ES vartotojams arba sistemingai stebi interneto vartotojų elgesį, tiek kiek jų elgesys vyksta ES.
4. Didžiųjų duomenų analizės prigimtis duomenis rinkti iš karto neapibrėžtiems tikslams bei aptikti netikėtas koreliacijas yra ribojama tikslo apribojimo principu, esančiu vienu iš privalomų BDAR reikalavimų. Didžiųjų duomenų organizacijų tikslams, kurie nesuderinami su pirminiu duomenų tikslu, organizacijos privalo gauti pakartotinį duomenų subjekto sutikimą, tačiau sutikimas bet kada gali būti atšaukiamas, o mašininio mokymosi technologijų specialistų bendruomenė tik neseniai pradėjo tyrimus siekiant galutinai išsiaiškinti, kaip atskirų rezultatų ištrynimas paveiks didžiųjų duomenų analizės jau gautas išvadas.
5. Duomenų kiekio mažinimo principas, esantis privalomu BDAR reikalavimu, taip pat laikomas ribojančiu didžiųjų duomenų analizės pranašumus, kadangi ribojamos galimybės iš visų įmanomų surinktų duomenų atrasti pažangius rezultatus. Šios problemos sprendimo būdas gali būti duomenų anonimizavimas, tačiau tik tuomet, kai duomenų valdytojas užtikrina, jog asmens duomenys negalėtų būti vėl identifikuoti ir susieti su

asmeniu, taip pat, kai didžiųjų duomenų analizės tikslams pasiekti nereikia asmenis identifikuojančių duomenų.

6. BDAR neužkerta kelio automatizuotų sprendimų, įskaitant profiliavimą, priėmimui. Viena iš diskriminacijos rūšių, galinčių pasireikšti algoritminio profiliavimo metu, yra netiesioginė diskriminacija, kuomet dėl neutralių faktų apie asmenis, tam tikra asmenų grupė yra nepalankiau vertinama dėl vienos ar kelių jų specialiųjų kategorijų duomenų. Organizacijos yra raginamos audituoti algoritmus, kad būtų išvengta diskriminuojančio pobūdžio automatizuotų sprendimų, tačiau algoritmų galimybės atrasti vis naujas koreliacijas kelia į ateitį orientuotus iššūkius, kadangi algoritmai gali atrasti naujų netiesioginės diskriminacijos formų, todėl neaišku, ar tokioms situacijoms visuomet iš anksto bus pasiruošę algoritminiai auditai.
7. BDAR nustato atvejus, kuriais organizacijos, prieš pradedančios užsiimti nauja technologijų veikla, turi atlikti poveikio duomenų apsaugai vertinimą. Didžiųjų duomenų kontekste šio vertinimo poreikio pagrindinė priežastis yra didžiųjų duomenų analizės veikla, kurios metu automatinėmis priemonėmis atliekamas asmeninių savybių vertinimas. Poveikio duomenų apsaugai vertinimo metu galima aptikti pavojus, kuriuos galėtų kelti naujų didžiųjų duomenų analizės technologijų taikymas asmens duomenims, taip pat nustatyti, kokių priemonių duomenų valdytojai turi imtis, norėdami sumažinti šių pavojų apimtį.

ŠALTINIŲ SĄRAŠAS

Specialioji literatūra

1. Aggarwal, J.V., Bhatnagar, V., Mishra, D.K. (2018). Big data analytics. *Springer Singapore*. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://link.springer.com/book/10.1007%2F978-981-10-6620-7
2. Ajibade , O. A. (2018). Critical Appraisal of Big Data Analytics within the General Data Protection Regulation (GDPR) Landscape [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: DOI:10.13140/RG.2.2.18365.31207
3. Altman, M., Wood, A., O'Brien, D.R., Gasser, U. (2018). Practical approaches to big data privacy over time. *International Data Privacy Law*, 8, 1, 29–51, [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipx027
4. Araujo, T., Helberger, N., Kruikemeier, S., De Vreese, C.H. (2020). In AI we trust? Perceptions about automated decision-making by artificial intelligence. *AI & SOCIETY*, *35*(3), 611-623. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://link.springer.com/article/10.1007/s00146-019-00931-w
5. Brkan, M. (2019). Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond. *International journal of law and information technology*, *27*(2), 91-121. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/ijlit/eay017
6. Castets-Renard, C. (2019). Accountability of Algorithms in the GDPR and beyond: A European Legal Framework on Automated Decision-Making. *Fordham Intell. Prop. Media & Ent. LJ*, *30*, 91. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://heinonline.org/HOL/LandingPage?handle=hein.journals/frdipm30&div=8&id=&page
7. Colangelo, G., Maggiolino, M. (2018). Data accumulation and the privacy–antitrust interface: insights from the Facebook case. *International Data Privacy Law*, *8*(3), 224-239. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipy018

8. Custers, B., Uršič, H. (2016). Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International data privacy law*, *6*(1), 4-15. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipv028
9. D' Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.A., Bourka, A. (2015). Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. *arXiv preprint arXiv:1512.06000*. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://arxiv.org/abs/1512.06000
10. De Hert, P., Czerniawski, M. (2016). Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. *International Data Privacy Law*, *6*(3), 230-243. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipw008
11. De Hert, P., Papakonstantinou, V. (2020). Framing Big Data in the Council of Europe and the EU data protection law systems: Adding 'should'to 'must'via soft law to address more than only individual harms. *Computer Law & Security Review*, [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1016/j.clsr.2020.105496
12. De Hert, P., Papakonstantinou, V., Malgieri, G., Beslay, L., Sanchez, I. (2018). The right to data portability in the GDPR: Towards user-centric interoperability of digital services. *Computer law & security review*, *34*(2), 193-203. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1016/j.clsr.2017.10.003
13. De Hert, P., Sajfert, J. (2019). Regulating Big Data in and out of the Data Protection Policy Field [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://pure.uvt.nl/ws/portalfiles/portal/32291967/pdh19_js_EDPL_big_data.pdf
14. Devins, C., Felin, T., Kauffman, S., Koppl, R. (2017). The law and big data. *Cornell JL & Public Policy*, *27*, 357. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://scholarship.law.cornell.edu/cjlpp/vol27/iss2/3
15. Erdos, D., Garstka, K. (2019). The 'Right to be Forgotten' Online within G20 statutory data Protection Frameworks. *International Data Privacy Law*, 10, 4, 294–313 [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipaa012
16. Europos Sąjungos pagrindinių teisių agentūra, Europos Taryba (2018). Handbook on European Data protection Law. *Publications Office of the European Union* [interaktyvus. Žiūrėta 2021

m. balandžio 3 d.]. Prieiga per internetą: https://op.europa.eu/en/publication-detail/-/publication/5b0cfa83-63f3-11e8-ab9c-01aa75ed71a1/language-en

17. Finck, M., Biega, A. (2021). Reviving Purpose Limitation and Data Minimisation in Personalisation, Profiling and Decision-Making Systems. *Max Planck Institute for Innovation & Competition Research Paper*, 21-04. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: http://dx.doi.org/10.2139/ssrn.3749078
18. Finck, M., Pallas, F. (2020). They who must not be identified-distinguishing personal from non-personal data under the GDPR. *Forthcoming, International Data Privacy Law*, 19-14. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: http://dx.doi.org/10.2139/ssrn.3462948
19. Forgó, N., Hänold, S., Schütze, B. (2017). The principle of purpose limitation and big data. In *New technology, big data and the law*,17-42. Springer, Singapore. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1007/978-981-10-5038-1_2
20. Gandomi, A., Haider, M., 2015. Beyond the hype: Big data concepts, methods, and analytics. *International journal of information management*, 137-144. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1016/j.ijinfomgt.2014.10.007
21. Globocnik, J. (2020). The Right to Be Forgotten is Taking Shape: CJEU Judgments in GC and Others (C-136/17) and Google v CNIL (C-507/17). *GRUR international*, *69*(4), 380-388. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/grurint/ikaa002
22. Goodman, B., Flaxman, S. (2017). European Union regulations on algorithmic decision-making and a "right to explanation". *AI magazine* [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ojs.aaai.org/index.php/aimagazine/article/view/2741
23. Ishii, K. (2018). Discussions on the Right to Data Portability from Legal Perspectives. In *IFIP International Conference on Human Choice and Computers*, 338-355. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://link.springer.com/chapter/10.1007/978-3-319-99605-9_26
24. Organisation for Economic Co-operation and Development (2013). *Exploring Data-Driven Innovation as a New Source of Growth: Mapping the Policy Issues Raised by" Big Data"*. OECD Publishing. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://www.oecdilibrary.org/docserver/5k47zw3fcp43en.pdf?expires=1617776347&id=id&accname=guest&checksum=F2990C8A131B134FF4063312C83B70BF

25. Kaminski, M.E., Malgieri, G. (2019). Algorithmic impact assessments under the GDPR: producing multi-layered explanations. *International Data Privacy Law*,020 [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipaa020
26. Kuner, C., Cate, F.H., Millard, C., Svantesson, D.J.B. (2012). The challenge of 'big data'for data protection. 2, 2, 47–49, [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ips003
27. Krishnamurthy, V. (2020) A Tale of Two Privacy Laws: The GDPR and the International Right to Privacy. *Cambridge University Press*, 26-30. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1017/aju.2019.79
28. Mittelstadt, B. (2016). Automation, algorithms, and politics| Auditing for transparency in content personalization systems. *International Journal of Communication*, *10*, 12. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ijoc.org/index.php/ijoc/article/view/6267
29. Patgiri, R., Ahmed, A. (2016). Big data: The v's of the game changer paradigm. In *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)* 17-24. IEEE. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ieeexplore.ieee.org/document/7828355
30. Rhoen, M., Feng, Q.Y. (2018). Why the 'Computer says no': illustrating big data's discrimination risk through complex systems science. *International data privacy law*, *8*(2), 140-159. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipy005
31. Rubinstein, I. (2013). Big data: the end of privacy or a new beginning?. *International Data Privacy Law*, 74-87. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ips036
32. Selbst, A., Powles, J. (2017). "Meaningful Information" and the Right to Explanation. *International Data Privacy Law*, 7, 4, 233–242 [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipx022
33. Tene, O., Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.* [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.] Prieiga per internetą: https://scholarlycommons.law.northwestern.edu/njtip/vol11/iss5/1/

34. Villaronga, E.F., Kieseberg, P., Li, T. (2018). Humans forget, machines remember: Artificial intelligence and the right to be forgotten. *Computer Law & Security Review*, *34*(2), 304-313. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1016/j.clsr.2017.08.007
35. Voigt, P. and Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10, 3152676. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://www.worldcat.org/title/eu-general-data-protection-regulation-gdpr-a-practical-guide/oclc/1001382746
36. Wachter, S., Mittelstadt, B., Russell, C. (2020). Why fairness cannot be automated: Bridging the gap between EU non-discrimination law and AI. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: http://dx.doi.org/10.2139/ssrn.3547922
37. Veale, M., Edwards, L. (2018). Clarity, surprises, and further questions in the Article 29 Working Party draft guidance on automated decision-making and profiling. *Computer Law & Security Review*, 34(2), 398-404. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://doi.org/10.1016/j.clsr.2017.12.002
38. Zuiderveen Borgesius, F. (2018). Discrimination, artificial intelligence, and algorithmic decision-making. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://dare.uva.nl/search?identifier=7bdabff5-c1d9-484f-81f2-e469e03e2360
39. Zaleskis, J. (2019). *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Monografija. Vilnius: VĮ Registrų centras.
40. Zarsky, T.Z. (2004). Desperately seeking solutions: using implementation-based solutions for the troubles of information privacy in the age of data mining and the internet society. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://digitalcommons.mainelaw.maine.edu/cgi/viewcontent.cgi?article=1416&context=mlr
41. Zarsky, T.Z. (2017). Incompatible: the GDPR in the age of big data. *Seton Hall L. Rev.*, 47, 995. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1606&context=shlr

Teisės norminiai aktai

Tarptautinės sutartys

1. Visuotinė žmogaus teisių deklaracija (1948). *Valstybės žinios*, 2006, 68-2497.
2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (1950). *Valstybės žinios,* 1995, Nr. 40-987.
3. Tarptautinis pilietinių ir politinių teisių paktas (1966) *Valstybės žinios*, 2002, Nr. 77-3288.
4. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) (1981) *Valstybės žinios*, 2001, Nr. 32-1059.

Europos Sąjungos teisės norminiai aktai

1. Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, OL L 281.
2. Europos Parlamento ir Tarybos 2002 m. liepos 12 d. direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL L 201, 2002 7 31,. 37–47.
3. Europos Sąjungos pagrindinių teisių chartija (2012) OL C 326, 2012 10 26, p. 391-407.
4. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OJ L 119.

Lietuvos teisės norminiai aktai

1. Lietuvos Respublikos Konstitucija. *Valstybės žinios*, 1992, nr. 33-1014.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas (2018). *TAR*, 11733.
3. Duomenų tvarkymo operacijų, kurioms taikomas reikalavimas atlikti poveikio duomenų apsaugai vertinimą, sarašas (2019) *TAR, 2019-03-14, Nr. 4104,* 1T-35 (1.12.E).

***Soft law* šaltiniai**

1. ES 29 str. duomenų apsaugos darbo grupė (2010). Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“, vasario 16 d. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.] Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf
2. Information Commissioner‘s Office (2014). Big data and data protection [interaktyvus. Žiūrėta 2021 m. balandžio 5 d.]. Prieiga per internetą: https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220
3. Jourová, V. (2016). The EU Data Protection reform and Big Data [interaktyvus. Žiūrėta 2021 m. balandžio 3d.] Prieiga per internetą: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=41523
4. Council, O.E. (2017). Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data. *T-PD 1,* .23. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://rm.coe.int/16806ebe7a
5. ES 29 str. duomenų apsaugos darbo grupė (2017). Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės, spalio 3 d. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.
6. ES 29 str. duomenų apsaugos darbo grupė (2017). Gairės dėl sutikimo pagal Reglamentą 2016/679, lapkričio 28 d. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=623051
7. ES 29 str. duomenų apsaugos darbo grupė (2017). Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės, lapkričio 29 d. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://www.teismai.lt/data/public/uploads/2020/02/20180411_skaidrumo_uztikrinimo_gaires.pdf
8. Information Commissioner‘s Office (2017). Big data, artificial intelligence, machine learning and data protection [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and dataprotection.pdf

9. European Data Protection Board (2018). European Data Protection Board rules of procedures [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_rop2_adopted_23112018_en.pdf.pdf

Teismų praktika

1. *Debra Allonby* prieš *Accrington & Rossendale College, Education Lecturing Services, trading as Protocol Professional ir Secretary of State for Education and Employment* [ESTT], Nr. C-256/01 [2004 m. sausio 13 d] ECLI:EU:C:2004:18
2. *Google Spain* ir *Google* [ESTT], Nr. C-131/12, [2014 m. gegužės 13 d.]. ECLI:EU:C:2014:317.

Kiti šaltiniai

1. 2018 m. gegužės 25 d. None of Your Business skundas dėl Facebook Ireland Ltd. [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: complaint-facebook.pdf (noyb.eu)
2. Telegram.org. *Moving Chat History from Other Apps* (modifikuota 2021). [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://telegram.org/blog/move-history
3. https://datatransferproject.dev. *Data Transfer Project* [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://datatransferproject.dev/what-is-dtp
4. https://transparencyreport.google.com. *Google Transparency Report* [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://transparencyreport.google.com/eu-privacy/overview
5. https://www.compliancejunction.com. *Danish DPA Issues First Ever GDPR Fine Against Taxi Company* (modifikuota 2019-04-24) [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://www.compliancejunction.com/danish-dpa-issues-first-ever-gdpr-fine-against-taxi-company/
6. gdpr.eu. *Data anonymization and GDPR compliance: the case of Taxa 4 x 35* [interaktyvus. Žiūrėta 2021 m. balandžio 3 d.]. Prieiga per internetą: https://gdpr.eu/data-anonymization-taxa-4x35/

SANTRAUKA

Didžiųjų duomenų (*big data*) reguliavimas pagal ES Bendrąjį duomenų apsaugos reglamentą

Augustė Abukauskaitė

Magistro darbe nagrinėjamas ES Bendrojo duomenų apsaugos reglamento nuostatų taikymas didiesiems duomenims. Pirmoje darbo dalyje atskleidžiama didžiųjų duomenų ir didžiųjų duomenų analizės samprata. Pirmoji magistro darbo dalis taip pat apima didžiųjų duomenų ir duomenų apsaugos teisės ir sąveiką. Aptariami pagrindiniai tarptautinės, Europos Sąjungos ir Lietuvos teisės privatumo ir duomenų apsaugos šaltiniai, reglamentuojantys didžiųjų duomenų reguliavimą. Antroje darbo dalyje dėmesys skiriamas bendrųjų reglamento nuostatų taikymui. Didžiųjų duomenų kontekste aptariami reglamento tikslai ir dalykas, teritorinis reglamento taikymas, ypatingą apsaugos garantiją turintys specialiųjų kategorijų asmens duomenys bei duomenų valdytojo ir tvarkytojo samprata. Trečioje darbo dalyje pažymima, jog norint praktikuoti didžiųjų duomenų technologijas, reikalinga laikytis duomenų apsaugos teisės principų. Darbe aptariami teisėtumo, sąžiningumo ir skaidrumo, duomenų tikslo apribojimo, duomenų kiekio mažinimo, tikslumo principai. Šioje dalyje atskleidžiami principų taikymo didiesiems duomenims probleminiai aspektai. Ketvirtoji darbo dalis skirta labiausiai analizuojamoms ir didžiausius probleminius iššūkius ir neaiškumus keliančioms duomenų subjektų teisėms, įskaitant teisę susipažinti su tvarkomais duomenimis, teisę į duomenų perkeliamumą, teisę reikalauti ištrinti duomenis („teisę būti pamirštam“) bei automatizuotą sprendimų priėmimą, įskaitant profiliavimą. Ketvirtoje dalyje taip pat aptariamas poveikio duomenų apsaugai vertinimas kaip dažnai reikalaujama didžiųjų duomenų technologijų privatumo rizikos mažinimo priemonė.

SUMMARY

Regulation of Big Data under the EU General Data Protection Regulation

Augustė Abukauskaitė

The master‘s thesis examines the application of the provisions of the EU General Data Protection Regulation to Big Data. The first part of the thesis includes the concept of big data and big data analytics. The first part also reveals the interaction between big data and data protection. Moreover, this paper includes analysis of international, European Union, and Lithuanian sources of privacy and data protection law governing the regulation of big data and big data analytics. The second part of the master‘s thesis focuses on applying the Regulation's general provisions, including the objectives and subject matter of the Regulation, the territorial scope, the essence of special categories data, and the concept of the data controller and data processor. The third part of the thesis indicates that big data technologies' practice requires compliance with the principles of GDPR. Attention is paid to the principles of lawfulness, fairness, transparency, and the principles of data purpose limitation, data minimisation, and accuracy. The fourth section focuses on the most analyzed and problematic data subjects' rights, including access to the personal data, the right to data portability, the right to erasure ("right to be forgotten"), and automated decision-making, including profiling. The fourth section also discusses data protection impact assessment as an often required privacy risk mitigation tool for large data technologies.