Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Arno Malakausko
V kurso, tarptautinės ir Europos Sąjungos teisės
studijų šakos studento

Magistrinis darbas

Automatizuotas sprendimų priėmimas pagal BDAR 22 straipsnį ir dirbtinis intelektas: taikymo prielaidos ir problematika

Automated Decision Making under Article 22 of the GDPR and Artificial Intelligence: Application Prerequisites and Issues

Vadovas: Asist. dr. Donatas Murauskas

Recenzentė: Asist. dr. Deimilė Prapiestytė

Kaunas
2022

TURINYS

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojamas BDAR 22 straipsnis: jo taikymo prielaidos ir problemos, kylančios duomenų valdytojams, savo veikloje pasitelkiantiems dirbtinio intelekto (DI) įrankius. Darbe analizuojamos automatizuotų sprendimų ir profiliavimo sąvokos, BDAR 22 straipsnio taikymo turinys bei ribos. Darbe atskleidžiama BDAR 22 straipsnio 3 dalyje įtvirtintų tinkamų duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonių užtikrinimo naudojant DI problematika. Darbe analizuojamas teisės gauti paaiškinimą (ne)egzistavimo klausimas ir įtaka duomenų valdytojams, naudojantiems DI.

Pagrindiniai žodžiai: profiliavimas, automatizuotų sprendimų priėmimas, dirbtinis intelektas, teisė gauti paaiškinimą.

This paper analyses Article 22 of the GDPR: the prerequisites for its application, and the issues related to the application of this Article to data controllers using artificial intelligence (AI) in their activities. It analyses the concepts of automated decision making and profiling, also the content and limits of the application of Article 22 of the GDPR. The work highlights the issue of ensuring suitable measures to safeguard the data subject's rights, freedoms and legitimate interests (as set out in Article 22(3) of the GDPR) in the use of AI. The work analyses the issue of the (non)existence of the right to an explanation and its impact on data controllers using AI.

Key words: profiling, automated decision making, artificial intelligence, right to an explanation.

SANTRUMPOS

Temos specifiškumas ir duomenų apsaugos teisės sąvokų autonomiškumas nulemia tai, kad visų pirma, yra tikslinga apsibrėžti šias sąvokas ir pateikti jų santrumpas:

- **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.
- **BDAR –** 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
- **DI (dirbtinis intelektas)** – šio darbo tikslams pasiekti DI turėtų būti suprantamas pačia bendriausia (plačiausia) prasme, kaip mašinos, kurios atlieka funkcijas, kurioms atlikti reikia intelekto, kai jas atlieka žmonės (McCarthy et al.. 2006, p. 11), pavyzdžiui, pokalbių robotai, virtualūs asistentai, gilaus mokymosi ir mašininio mokymosi algoritmai, naudojami įvairiose interneto srityse, pavyzdžiui, paieškoje ir socialinėse medijose. Pažymėtina, kad šiame darbe vartojama sąvoka DI apima tik tas DI technologijas, kurios atlikdamos funkcijas tvarko asmens duomenis.
- **Duomenų subjektas** – fizinis asmuo, kurio asmens duomenys yra tvarkomi. Plačiau ši sąvoka aiškinama šio darbo 2.2.1 poskyryje.
- **Duomenų valdytojas** – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise.
- **Duomenų tvarkymas** – bet kokia automatizuotomis arba neautomatizuotomis priemonėmis su asmens duomenimis ar asmens duomenų rinkiniais atliekama operacija ar operacijų seka, kaip antai rinkimas, įrašymas, rūšiavimas, sisteminimas, saugojimas, adaptavimas ar keitimas, išgava, susipažinimas, naudojimas, atskleidimas persiunčiant,

platinant ar kitu būdu sudarant galimybę jais naudotis, taip pat sugretinimas ar sujungimas su kitais duomenimis, apribojimas, ištrynimas arba sunaikinimas.

- **EDAV –** Europos duomenų apsaugos valdyba.
- **EK** – Europos Komisija.
- **ES** – Europos Sąjunga.
- **ESTT** – Europos Sąjungos teisingumo teismas.
- **ES Duomenų apsaugos direktyva** – 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.
- **ES teisėsaugos duomenų apsaugos direktyva** – 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos Direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR.
- **Specialiųjų kategorijų asmens duomenys –** asmens duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus ar narystę profesinėse sąjungose, genetiniai duomenys, biometriniai duomenys, sveikatos duomenys arba duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją.
- **Priežiūros institucija** – valstybės narės pagal BDAR 51 straipsnį įsteigta nepriklausoma valdžios institucija.

ĮŽANGA

Dėl sparčios technologinės plėtros ir globalizacijos kyla naujų asmens duomenų apsaugos sunkumų. Žymiai išaugo asmens duomenų rinkimo ir keitimosi jais mastas. Technologijos leidžia privačioms bendrovėms ir valdžios institucijoms vykdant savo veiklą naudotis asmens duomenimis precedento neturinčiu mastu (BDAR preambulės 6 punktas). Statistika rodo, kad 2010–2020 m. naudojamų duomenų kiekis padidėjo nuo 1,2 trilijono gigabaitų iki beveik 60 trilijonų gigabaitų t. y. duomenų kiekis auga eksponentiškai (Forbes, n.d.). Tokio plataus masto duomenų (įskaitant ir asmens duomenų) tvarkymas gali kelti pavojus tiek individualiems asmenims, tiek įvairioms fundamentalioms visuomenės gyvavimo sąlygoms, pavyzdžiui, demokratiniams procesams[1].

Visgi, vertinant iš duomenų tvarkymo kylančius pavojus ir jų užkardymo priemones, nereikėtų pamiršti ir naudos, kurią suteikia duomenų tvarkymas. ES teisės aktų leidėjas pripažįsta, kad asmens duomenys turėtų būti tvarkomi taip, kad tai pasitarnautų žmonijai. Teisė į asmens duomenų apsaugą nėra absoliuti; ji turi būti vertinama atsižvelgiant į jos visuomeninę paskirtį ir derėti su kitomis pagrindinėmis teisėmis, remiantis proporcingumo principu. Šiuo reglamentu paisoma visų Chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, visų pirma <...> laisvės užsiimti verslu (BDAR preambulės 3 punktas).

DI yra paremtas plataus masto duomenų (dažnu atveju – asmens duomenų) tvarkymu (Sartor, 2020, p. 1) ir šios technologijos taikymas gali atnešti įvairialypės naudos visuomenei, pavyzdžiui, dirbtinio intelekto technologijų naudojimas gali padėti gydytojams nustatyti tikslesnę ligos diagnozę[2] ir taikyti individualizuotą gydymą; įmonės gali numatyti rinkos tendencijas ir priimti veiksmingus sprendimus; vartotojai gali gauti individualizuotas paslaugas; valdžios institucijos gali optimizuoti viešųjų gėrybių (angl. *public goods*) valdymą ir koordinuoti piliečių veiksmus (pvz. eismo, energetikos, komunalinių paslaugų valdymo srityse) (Sartor, 2020, p. 18).

EK komunikate „Dirbtinis intelektas Europai“ teigiama, kad yra visos sąlygos ES remiantis savo vertybėmis tapti DI revoliucijos lydere (toliau – Komunikatas) (Dirbtinis intelektas Europai, 2018, p. 20). Visgi, 2018 m. gegužės 25 dieną įsigaliojus BDAR, tokia Komunikate pateikiama pozicija yra pagrindo suabejoti. Remiantis statistiniais

[1] Dar 2018 m. plačiai nuskambėjo įvykis, kuomet pasklido informacija, kad per 2016 m. JAV prezidento rinkimus, D. Trumpo rinkimų štabui dirbanti kompanija „Cambridge Analytica“ naudojo daugiau nei 50 mln. *Facebook* vartotojų duomenis juos pasitelkiant kandidato reklamai, tokiu būdu galimai paveikiant šių vartotojų pasirinkimą prezidento rinkimuose (the Guardian, 2018).

[2] Pavyzdžiui, viename tyrime dirbtinio intelekto modelis, naudojantis algoritmus ir gilųjį mokymąsi (angl. *deep learning*), diagnozavo krūties vėžį tiksliau nei vienuolikos patologų komanda (Bejnordi et al., 2017).

duomenimis, nuo BDAR įsigaliojimo ES priežiūros institucijų už BDAR pažeidimus paskirtų baudų suma siekia daugiau nei pusantro milijardo eurų (www.enforcementtracker.com, n.d.). Griežti, dažnu atveju abstraktaus pobūdžio BDAR reikalavimai bei didelių baudų rizika[3] gali atgrasyti įmones, ypatingai mažas ir vidutines[4] nuo DI technologijų kūrimo bei diegimo savo veikloje.

Aktualumas. K. Koerner nuomone, jei ES nespręs iš BDAR kylančių iššūkių DI kontekste, BDAR trukdys DI plėtrai ir naudojimui Europoje, todėl Europos įmonėms iškils nepalanki konkurencinė padėtis besiformuojančioje pasaulinėje algoritminėje ekonomikoje[5] (angl. *algorithmic economy)* (Koerner, 2018).

BDAR preambulės 7 punkte teigiama, kad fiziniai asmenys turėtų kontroliuoti savo asmens duomenis ir turėtų būti užtikrintas didesnis teisinis ir praktinis tikrumas fiziniams asmenims, ekonominės veiklos vykdytojams ir valdžios institucijoms. Taigi, Europos Sąjungos teisės aktų leidėjas pripažįsta duomenų apsaugos teisės teisinio ir praktinio tikrumo (aiškumo) svarbą ne tik fiziniams asmenims, bet ir ekonominės veiklos vykdytojams bei valdžios institucijoms. BDAR yra būdingas abstraktumas, dėl kurio duomenų valdytojams praktikoje kyla iššūkių siekiant identifikuoti žingsnius, kuriuos jie turėtų atlikti tam, kad būtų išvengta BDAR pažeidimų ir gresiančių baudų.

BDAR 22 straipsnio turinys ir taikymo sritis nulemia tai, kad šis straipsnis yra ypač svarbus duomenų valdytojams, kurie atlieka duomenų tvarkymą pasitelkdami DI technologijas, todėl svarbu atlikti mokslinius tyrimus, nukreiptus į šio BDAR straipsnio analizę, siekiant nustatyti šio straipsnio turinį bei identifikuoti šio straipsnio taikymo DI naudotojams probleminius aspektus.

Tikslas. Šio darbo tikslas yra išanalizuoti BDAR 22 straipsnio taikymo duomenų valdytojams, savo veikloje naudojantiems DI, prielaidas bei problematiką.

Uždaviniai. Tikslui įgyvendinti keliami šie uždaviniai:

1) Nurodyti automatizuotų sprendimų priėmimo ir profiliavimo sąvokų turinį.
2) Išanalizuoti BDAR 22 straipsnio sudėtį ir jo taikymo ribas.

---

[3] Priklausomai nuo pažeistos BDAR nuostatos, gali būti skiriamos administracinės baudos iki 10 000 000 EUR arba, įmonės atveju – iki 2 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė (BDAR 83 str. 4 d.) arba 20 000 000 EUR arba, įmonės atveju – iki 4 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė (BDAR 83 str. 5 d.).

[4] Mažos ir vidutinės įmonės, tai tokios įmonės, kuriose dirba mažiau nei 250 darbuotojų. Čia jos išskiriamos todėl, nes lyginant su didelėmis įmonėmis, resursai, kurie būtų skirti įvertinti ir užkardyti iš asmens duomenų tvarkymo kylančias rizikas, yra (labiau) riboti.

[5] 2018 m. atliktame tyrime buvo apskaičiuota, kad dėl spartėjančios dirbtinio intelekto plėtros ir naudojimo pasaulinis BVP iki 2030 m. gali padidėti iki 14 % (15,7 trilijono JAV dolerių) (Gillham, 2018, p. 3). Šie skaičiai iliustruoja DI ekonominį potencialą bei DI plėtros užtikrinimo svarbą.

3) Atskleisti duomenų subjektų teisių, laisvių ir teisėtų interesų užtikrinimo problematiką DI naudojimo kontekste.
4) Aptarti teisės gauti paaiškinimą (ne)egzistavimo problemą bei iš šios teisės kylančias implikacijas DI naudojimui.

Objektas. Darbo objektas yra BDAR 22 straipsnio taikymo duomenų valdytojams, savo veikloje naudojantiems DI technologijas, prielaidos ir apimtis. BDAR 22 straipsnis yra taip pat minimas kitose nukreipiančio pobūdžio BDAR normose[6], tačiau šiame darbe šios normos nėra analizuojamos, t. y. koncentruojamasi tik į BDAR 22 straipsnio analizę. Duomenų valdytojams, savo veikloje naudojantiems DI technologijas yra taikomi visi kiti (bendrieji) BDAR reikalavimai, tačiau šie reikalavimai nėra šio darbo objektas. Šiame darbe taip pat nėra analizuojama DI sąvoka, kadangi ji plačiai nagrinėta kitų autorių darbuose.

Metodika. BDAR 22 straipsnis šiame darbe nagrinėjamas atsižvelgiant į BDAR tikslą – siekį apginti duomenų subjektus nuo iš duomenų tvarkymo kylančių pavojų, tuo pačiu atsižvelgiant į tai, kad teisė į duomenų apsaugą nėra absoliuti ir ji turi būti balansuojama su, *inter alia*, laisve užsiimti verslu (BDAR preambulės 4 punktas). BDAR 22 straipsnis nagrinėjamas sistemiškai su kitomis BDAR nuostatomis (neizoliuotai), ypač atsižvelgiant į tai, kad BDAR reguliavimo pamatą sudaro principai (BDAR 5 str.), kurių veikimas turi būti užtikrintas viso duomenų tvarkymo ciklo metu. BDAR 22 straipsnio 1 dalies pažodinė formuluotė „duomenų subjektas turi teisę“ yra lyginama su *soft law* šaltiniuose ir teisės mokslo doktrinos atstovų darbuose išreiškiama pozicija, kad BDAR 22 straipsnis įtvirtina ne teisę, bet bendrą draudimą. Automatizuotų sprendimų priėmimo ir profiliavimo sąvokos nagrinėjamos, *inter alia*, istoriniu požiūriu, atsakant į klausimą, ar BDAR pirmtakėje ES duomenų apsaugos direktyvoje šios sąvokos (ne)buvo įtvirtintos ir kodėl.

Originalumas. Tiek užsienio, tiek Lietuvos teisėtyroje, išsamios BDAR 22 straipsnio analizės, ją susiejant su DI naudojimo kontekste kylančiais ypatumais, nėra. Lee A. Bygrave (Kuner, Bygrave and Docksey, 2019), D. Sancho (Sancho, 2020) savo darbuose apžvelgia BDAR 22 straipsnį bendrąja prasme. M. Brkan (Brkan, 2017) straipsnyje analizuoja BDAR ir ES Teisėsaugos duomenų apsaugos direktyvos reikalavimus, susijusius su automatizuotų sprendimų priėmimu, taip pat apžvelgia būdus, kaip būtų galima užtikrinti tokių sprendimų skaidrumą. E. Falleti (Falleti, 2019), B. Goodman ir S. Flaxman (Goodman ir Flaxman, 2017), L Tosoni (Tosoni, 2021), (S. Wachter et. al. (Watcher et. al., 2017) savo darbuose nagrinėja teisės į paaiškinimą (ne)egzistavimo

[6] BDAR 12 str. 1, 2, 3, 5 d.; 13 str. 2 d. f p.; 14 str. 2 d. g p.; 15 str. 1 d. h p.; 23 str. 1 d.; 47 str. 2 d. e p.; 70 str. 1 d. f p.; 83 str. 5 d. b p.

klausimą. G. Sartor (Sartor, 2020) nagrinėja BDAR ir DI ryšį, DI taikomas BDAR nuostatas, pateikia pasiūlymus dėl DI ir BDAR suderinamumo.

DI klausimus BDAR kontekste nagrinėjo Oslo universiteto absolventas[7] magistriniame darbe tema „AI Ethics Through the Lens of GDPR" ir Talino technikos universiteto absolventai A. Kesa ir T. Kerikmäe magistriniame darbe tema „Artificial Intelligence And The GDPR: Inevitable Nemeses?". Lietuvoje panašiomis temomis magistro darbus rengė Vytauto Didžiojo universiteto studentas A. Aidukas 2018 m. apgynęs darbą tema „Data Privacy and Artificial Intelligence: Is General Data Protection Regulation the Right Regulation in the Age of Intelligent Machines?", Vilniaus universiteto absolventė A. Babayan 2018 m. parašiusi darbą tema „Dirbtinio intelekto iššūkis žmogaus teisių apsaugos sričiai: robotų statuso reguliavimas" bei K. Seliutaitė, kurios 2020 m. parašyto darbo tema yra „ES Bendrojo duomenų apsaugos reglamento taikymo dirbtiniam intelektui ypatumai".

Šis magistro darbas iš minėtos tarptautinės mokslinės doktrinos ir kitų darbų, rašytų panašiomis temomis, išsiskiria savo keliamais uždaviniais, darbų tikslais, darbo apimtimi. Šis magistro darbas taip pat išsiskiria ir nagrinėjamais šaltiniais, kadangi šios temos svarba lemia naujų, dar nenagrinėtų šaltinių atsiradimą. Naujų šaltinių analizė lemia ir skirtingas šiame darbe, lyginant su kitais darbais, prieinamas išvadas.

Svarbiausi šaltiniai. Šio darbo rengimui ypač svarbūs *soft law* šaltiniai – Europos duomenų apsaugos valdybos (ir jos pirmtakės 29 straipsnio darbo grupės) gairės, rekomendacijos ir nuomonės įvairiai BDAR klausimais. Dėl sąlyginai trumpo BDAR taikymo laikotarpio, teismų praktikos, nagrinėjančios DI ir BDAR klausimus, nėra gausu, todėl teismų praktika pateikiama tik atskirų BDAR reikalavimų analizėje. Darbe daugiausiai remiamasi M. Brkan, L. A. Bygrave, L. Tosoni, G. Sartor, L. Mendoza, J. Zaleskio ir kitų teisės doktrinos atstovų darbais. Darbo temos specifika lemia tai, kad darbo temos aktualumui ir tam tikrais atvejais, siekiant iliustruoti darbe išsakytus teiginius, remiamasi statistiniais šaltiniais, žiniasklaidoje pateikiama informacija.

[7] Autoriaus vardas, tikėtina, siekiant užtikrinti autoriaus asmens duomenų apsaugą, darbe nėra pateikiamas.

1. PROFILIAVIMAS IR AUTOMATIZUOTŲ SPRENDIMŲ PRIĖMIMAS

BDAR 22 straipsnis įtvirtina nuostatas, susijusias su automatizuotu atskirų sprendimų priėmimu, įskaitant profiliavimą:

22 straipsnis

Automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą

1. 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.

2. 1 dalis netaikoma, jeigu sprendimas: a) yra būtinas siekiant sudaryti arba vykdyti sutartį tarp duomenų subjekto ir duomenų valdytojo, 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; arba c) yra pagrįstas aiškiu duomenų subjekto sutikimu.

3. 2 dalies a ir c punktuose nurodytais atvejais duomenų valdytojas įgyvendina tinkamas priemones, kad būtų apsaugotos duomenų subjekto teisės bei laisvės ir teisėti interesai, bent teisė iš duomenų valdytojo reikalauti žmogaus įsikišimo, pareikšti savo požiūrį ir užginčyti sprendimą.

4. 2 dalyje nurodyti sprendimai negrindžiami 9 straipsnio 1 dalyje nurodytais specialių kategorijų asmens duomenimis, nebent taikomi 9 straipsnio 2 dalies a arba g punktai ir yra nustatytos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti.

Siekiant tolimesnės šio straipsnio ir jo taikymo DI technologijoms problematikos analizės, visų pirma tikslinga pateikti šių sąvokų paaiškinimus: 1) profiliavimas, 2) automatizuotas atskirų sprendimų priėmimas.

1.1. Profiliavimas

Terminas „profiliavimas" kilęs iš italų kalbos žodžio „profilare", kuris reiškia nubrėžti objekto kontūrą: būtent tokia yra profiliavimo tvarkant asmens duomenis idėja, t. y. remiantis turimais duomenimis apie atskirus asmenis ar grupes aprašyti ar numatyti jų bruožus ir polinkius (Sartor, 2020, p. 22).

Profiliavimo sąvoka (skirtingai nei automatizuotų sprendimų sąvoka) nebuvo vartojama BDAR pirmtakėje ES duomenų apsaugos direktyvoje. Tai galima paaiškinti, *inter alia,* tuo, kad profiliavimo sąvoka, atsižvelgiant į tuometinį technologijų išsivystymo lygį, dar nebuvo tokia aktuali. J. Fenelon teigimu, vis plačiau naudojant technologijas ir didėjant duomenų rinkimui (pavyzdžiui, didžiųjų duomenų analizei naudojant mašininį mokymąsi ir dirbtinį intelektą), prireikė sukurti teisines apsaugos priemones, kad būtų galima kontroliuoti, kaip duomenų valdytojai ir duomenų tvarkytojai naudoja surinktus asmens duomenis. Todėl BDAR buvo įvesta nauja profiliavimo sąvoka (Fenelon, 2020, p. 4).

BDAR apibrėžia profiliavimą kaip bet kokios formos automatizuotą asmens duomenų tvarkymą, kai asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti ar numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu (BDAR 4 straipsnio 4 punktas).

BDAR materialinė taikymo sritis apima tik asmens duomenų tvarkymą (BDAR 2 straipsnio 1 dalis), todėl ir profiliavimas BDAR kontekste turi būti suprantamas kaip procesas, apimantis ne duomenų (plačiąja prasme), bet būtent asmens duomenų tvarkymą. Naudojant profiliavimą iš (iš pažiūros) neaktualių asmens duomenų galima išvesti labai jautrią informaciją ir taip sudaryti išsamius ir tikslius asmenų profilius[8]. Profiliai vis

[8] Iliustravimui, galima pateikti praktikoje paplitusį tikslinės rinkodaros pavyzdį, kuomet įmonės, siekiančios optimizuoti kaštus, kreipiamus į produktų/paslaugų siūlymą potencialiems klientams, samdo išorės paslaugų teikėjus (pavyzdžiui *Google Ads*), kurie susiaurina asmenų, kuriems efektyviausia siūlyti produktus/paslaugas, ratą. Toks asmenų, kuriems efektyviausia siūlyti produktus/paslaugas, rato susiaurinimas vyksta pasitelkiant DI technologijas, kurios dėl savo gebėjimo apdoroti didelius duomenų kiekius gali, remiantis, *inter alia,* vartotojų naršymo internete duomenimis, pirkimų istorija, mygtuko „patinka“ paspaudimais socialinėse medijose ir kita informacija, profiliuoti tokius asmenis į tam tikras grupes ir padėti atsakyti į klausimą „kokia yra tikimybė, kad asmuo, su naršymo internete istorija X, pirkimų istorija Y ir mygtuko „patinka“ paspaudimais Z nupirks konkrečios įmonės konkretų produktą?“. Dar daugiau, atsakymai į tokius klausimus gali padėti įmonėms diferencijuoti produktų/paslaugų kainą pagal „profilį“ kuriam priskiriamas konkretus asmuo. Iš esmės tai reikštų, jog didėjant tikimybei, kad asmuo pirks produktą/paslaugą, didėtų ir atitinkamo produkto/paslaugos kaina.

dažniau naudojami priimant svarbius sprendimus, pradedant asmens kreditingumo vertinimu, baigiant įdarbinimu, policijos veikla ir nacionaliniu saugumu.

Iš BDAR 4 straipsnio 4 punkte pateikiamo apibrėžimo galima išskirti tokias profiliavimo sąvokos kumuliatyvias sąlygas: 1) bet kokios formos automatizuotas asmens duomenų tvarkymas; 2) siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus.

Kaip matyti, profiliavimas turi apimti bet kokios formos automatizuotą asmens duomenų tvarkymą.

BDAR 4 straipsnio 4 dalyje pateikiami žodžiai „bet kokios formos“ reiškia, kad profiliavimas turi apimti kokios nors formos automatizuotą duomenų tvarkymą, tačiau, remiantis apibrėžtimi, žmonės šiame procese taip pat gali dalyvauti (29 straipsnio darbo grupės gairės, 2018, p. 7). Pavyzdžiui, asmuo, siekiantis apsidrausti gyvybės draudimu, kreipiasi į draudimo bendrovę. Draudimo bendrovė savo internetiniame puslapyje prašo asmens atsakyti į tam tikrus klausimus, pavyzdžiui, koks yra asmens amžius, kokiomis ligomis asmuo serga, ar asmuo turi žalingų įpročių ir t. t. Remiantis šiais atsakymais, algoritmas priskiria asmenį į tam tikrą kategoriją. Asmens priskyrimas atitinkamai kategorijai lemia tai, koks draudimo pasiūlymas bus pateiktas asmeniui. Nors asmenį atitinkamam profiliui priskiria algoritmas, tačiau gali būti ir taip, kad galutinį sprendimą dėl asmens priskyrimo atitinkamai kategorijai gali priimti ir bendrovės darbuotojas.

Žodis „įvertinti“ rodo, kad profiliavimas apima tam tikros formos vertinimą arba sprendimo priėmimą dėl asmens (29 straipsnio darbo grupės gairės, 2018, p. 7). Šį teiginį taip pat iliustruoja aukščiau minimas gyvybės draudimo pavyzdys, kadangi pagal tai, kokiai kategorijai bus priskiriamas asmuo, atitinkamai bus nusprendžiama (įvertinama), kokio dydžio įmokas asmuo turės mokėti už savo gyvybės draudimą. Priešingai, jeigu duomenų valdytojas siekia suskirstyti savo klientus (pavyzdžiui, pagal amžių, lytį) tik statistiniais tikslais, nesiekdamas remiantis tokiais duomenimis priimti sprendimų ar vertinimų, tokia veikla nebus laikoma profiliavimu. Kaip teigia 29 straipsnio darbo grupė, profiliavimas <...> dažnai taikomas žmonių savybėms prognozuoti naudojant iš įvairių šaltinių gautus duomenis, siekiant padaryti kokias nors išvadas dėl asmens, remiantis kitų, statistiniu požiūriu panašių asmenų savybėmis. Apskritai profiliavimas reiškia informacijos apie asmenį (arba asmenų grupę) rinkimą ir asmens (–ų) savybių arba elgesio modelių vertinimą, norint jį arba juos priskirti tam tikrai kategorijai arba grupei, pirmiausia – siekiant išanalizuoti ir (arba) nuspėti aspektus, pvz., susijusius su: gebėjimu atlikti užduotį, interesais arba tikėtinu elgesiu.

Taigi, profiliavimo esmę sudaro asmens duomenų tvarkymas automatizuotu būdu siekiant išanalizuoti ir (arba) nuspėti aspektus, susijusius su profiliuojamu duomenų subjektu.

1.2. Automatizuotas sprendimų priėmimas

Automatizuotų sprendimų priėmimo sąvoka buvo vartojama ir ES duomenų apsaugos direktyvoje. Kaip teigia M. Brkan, nors priėmus BDAR šios nuostatos formuluotė iš esmės nepasikeitė, praktinė šios nuostatos svarba išaugo, nes su laiku vis dažniau naudojamasi automatizuotu sprendimų priėmimu (Brkan, 2018, p. 5). Automatizuotų sprendimų priėmimas, tai sprendimų priėmimas atliekamas automatizuotomis priemonėmis. Galima išskirti tokias automatizuotų sprendimų kategorijas:

1) Iš dalies automatizuoti sprendimai – kai sprendimas yra priimamas automatizuotomis priemonėmis, tačiau sprendimo priėmimo procese dalyvauja ir žmogus. Pavyzdžiui, bankas, paskolų suteikimo procese pasitelkia DI, kuris sugeneruoja asmens kredito reitingą pagal tam tikrus asmens duomenis, tvarkomus apie tą asmenį ir remiantis šiuo kredito reitingu pateikia pasiūlymą dėl paskolos dydžio ir sąlygų, tačiau galutinį sprendimą dėl paskolos suteikimo priima banko darbuotojas.
2) Tik automatizuotu duomenų tvarkymu grindžiami sprendimai – tai tokie atvejai, kai sprendimas yra priimamas be žmogaus įsikišimo. Šiuo atveju taip pat aktualus aukščiau minimas paskolos suteikimo sprendimo pavyzdys, tik šiuo atveju žmogus jame nedalyvautų (tik automatizuotu duomenų tvarkymu grindžiamų sprendimų sąvoka plačiau nagrinėjama šio darbo 2.2.2 poskyryje).

Automatizuoto sprendimų priėmimo taikymo sritis yra kitokia nei profiliavimo – automatizuotas sprendimų priėmimas gali būti vykdomas ir atliekant, ir jo neatliekant profiliavimą. Pavyzdžiui, baudų už greičio viršijimą skyrimas remiantis tik greičio matuoklių duomenimis yra automatizuoto sprendimų priėmimo procesas, kurio metu nebūtinai vykdomas profiliavimas. Tačiau, jei tam tikrą laiką būtų stebimi asmens vairavimo įpročiai ir, pvz., bauda būtų skiriama atsižvelgiant į kokį nors vertinimą, atliekamą atsižvelgiant ir į kitus veiksnius, pvz., į tai, ar greičio viršijimo pažeidimas padaromas pakartotinai ir ar vairuotojas neseniai nėra padaręs kitų kelių eismo taisyklių pažeidimų, toks sprendimas jau būtų grindžiamas profiliavimu (29 straipsnio darbo grupės gairės, 2018, p. 8).

Automatizuoti sprendimai gali būti priimami remiantis bet kokio pobūdžio duomenimis, pvz.: susijusių asmenų tiesiogiai suteiktais duomenimis (pvz., atsakymais į

klausimyną); stebint asmenis gautais duomenimis (pvz., programinės įrangos surinktais vietos nustatymo duomenimis); išvestiniais arba numanomais duomenimis, pvz., jau sudarytu asmens profiliu (pvz., kredito reitingu) (29 straipsnio darbo grupės gairės, 2018, p. 8).

Apibendrinant šio darbo 1 dalį, darytina išvada, kad automatizuotas sprendimų priėmimo sąvoka skiriasi nuo profiliavimo sąvokos. Automatizuotų sprendimų sąvoka yra susijusi su sprendimo dėl duomenų subjekto priėmimo būdu. Tuo tarpu profiliavimo sąvoka yra susijusi su asmens elgesio prognozavimu pagal tam tikras koreliacijas tarp duomenų, surinktų apie šį asmenį ir duomenų, turimų apie kitus asmenis. Nors automatizuotų sprendimo priėmimo sąvoką ir profiliavimo sąvoka galima vartoti kaip atskiras, tačiau dažnu atveju šios sąvokos papildo viena kitą t. y. automatizuoti sprendimai gali būti grindžiami profiliavimu ar iš dalies sutapti su profiliavimu.

2. TEISĖS NEBŪTI AUTOMATIZUOTAI PRIIMAMŲ SPRENDIMŲ SUBJEKTU TURINYS IR TAIKYMO RIBOS

BDAR 22 straipsnio 1 dalyje įtvirtinta, kad 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 (toliau – teisė nebūti automatizuotai priimamų sprendimų subjektu).

Siekiant išanalizuoti teisės nebūti automatizuotai priimamų sprendimų subjektu taikymo turinį, toliau bus nagrinėjamas BDAR 22 straipsnio 1 dalies dviprasmiškumo klausimas: „ar BDAR 22 straipsnio 1 dalyje yra įtvirtinta teisė, ar bendras draudimas?“ (šio darbo 2.1 skyrius) ir BDAR 22 straipsnio 1 dalies taikymo sąlygos (šio darbo 2.2 skyrius). Teisės nebūti automatizuotai priimamų sprendimų subjektu taikymo ribos bus nagrinėjamos analizuojant BDAR 22 straipsnio 2 dalyje įtvirtintas išimtis, kuomet minėta teisė, net ir atitikus visas sąlygas, nėra taikoma (šio darbo 2.3 skyrius). Šio darbo 2.4 skyriuje bus analizuojama specifika, susijusi su teisės nebūti automatizuotai priimamų sprendimų subjektu, kai yra tvarkomi specialiųjų kategorijų asmens duomenys.

2.1. Teisės nebūti automatizuotai priimamų sprendimų dviprasmiškumo problema

BDAR 22 straipsnio 1 dalyje įtvirtinta, kad 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.

Iš pirmo žvilgsnio gali atrodyti, kad BDAR 22 straipsnio 1 dalyje įtvirtinta formuluotė „duomenų subjektas turi teisę, kad jam nebūtų taikomas“ (o ne formuluotė „duomenų valdytojui draudžiama priimti“) implikuoja tai, kad duomenų subjektas, siekdamas pasinaudoti šia teise turėtų imtis aktyvių veiksmų, t. y. kreiptis į duomenų valdytoją dėl savo teisės įgyvendinimo. Nepaisant to, 29 straipsnio darbo grupė Gairėse dėl automatizuotų sprendimų priėmimo, išaiškino, kad BDAR 22 straipsnio 1 dalyje vartojama sąvoka „teisė“ nereiškia, kad 22 straipsnio 1 dalis taikoma tik tuomet, kai duomenų subjektas ja aktyviai pasinaudoja. 22 straipsnio 1 dalyje nustatytas bendras draudimas priimti sprendimus remiantis tik automatizuotu duomenų tvarkymu. Šis draudimas taikomas nepaisant to, ar duomenų subjektas imasi kokių nors veiksmų dėl su juo susijusių asmens duomenų tvarkymo (29 straipsnio darbo grupės gairės, 2018, p. 20). Tokį aiškinimą 29 straipsnio darbo grupė grindžia toliau nurodytais argumentais:

Pirma, aiškinimas, kad BDAR 22 straipsnio 1 dalyje įtvirtintas bendras draudimas sustiprina mintį, kad duomenų subjektas turi turėti galimybę kontroliuoti savo asmens duomenis, kaip įtvirtinta pagrindiniais BDAR principais. BDAR 22 straipsnį aiškinant kaip draudimą, o ne kaip teisę, kuria galima pasinaudoti, asmenys automatiškai apsaugomi nuo poveikio, kurį gali padaryti toks duomenų tvarkymas (29 straipsnio darbo grupės gairės, 2018, p. 21).

Antra, aiškinimą, kad BDAR 22 straipsnio 1 dalyje įtvirtintas bendras draudimas patvirtina BDAR preambulės 71 punktas, kuriame teigiama: „Tačiau tokiu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimų priėmimas turėtų būti leidžiamas, kai jis yra aiškiai leidžiamas Sąjungos ar valstybės narės teisėje <...> arba kai tai būtina sudarant arba vykdant <...> sutartį, arba tada, kai duomenų subjektas yra davęs aiškų sutikimą.“ Tai reiškia, kad BDAR 22 straipsnio 1 dalyje apibrėžtas duomenų tvarkymas paprastai nėra leidžiamas (29 straipsnio darbo grupės gairės, 2018, p. 21).

Trečia, nors BDAR III skyriuje nustatomos duomenų subjekto teisės, BDAR 12–22 straipsniai susiję ne tik su aktyviu naudojimusi teisėmis. Kai kurios iš šių teisių yra pasyvios: ne visos teisės yra susijusios su situacijomis, kai duomenų subjektas imasi kokių nors veiksmų, pavyzdžiui, pateikia kokį nors prašymą, skundą arba reikalavimą. BDAR 15–18 ir 20–21 straipsniai susiję su aktyviu duomenų subjekto naudojimusi savo teisėmis, o BDAR 13 ir 14 straipsniuose nustatytos prievolės, kurias duomenų valdytojas turi įvykdyti be aktyvaus duomenų subjekto įsikišimo. Taigi BDAR 22 straipsnis į šį skyrių įtrauktas ne siekiant suteikti aktyvią teisę (29 straipsnio darbo grupės gairės, 2018, p. 37).

Ketvirta, BDAR 22 straipsnis yra įtvirtintas skirsnyje „Teisė nesutikti ir automatizuotas atskirų sprendimų priėmimas“, taigi BDAR 22 straipsniu nėra suteikiama teisė nesutikti, kaip tai padaryta 21 straipsnyje (29 straipsnio darbo grupės gairės, 2018, p. 37).

Penkta, jei BDAR 22 straipsnį aiškintume kaip suteikiantį teisę nesutikti, BDAR 22 straipsnio 2 dalies c punkte nustatyta išimtis nebūtų labai prasminga. Pagal šią išimtį, automatizuotas sprendimų priėmimas gali būti vykdomas, jei duomenų subjektas duoda aiškų sutikimą. Tokiu atveju kiltų prieštaravimų, nes duomenų subjektas negali pareikšti ir nesutikimo, ir sutikimo dėl to paties duomenų tvarkymo (29 straipsnio darbo grupės gairės, 2018, p. 38).

Su aiškinimu, kad BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas, savo darbuose sutinka (eksplicitiškai arba implicitiškai) ir dauguma šio darbo autoriaus analizuotų duomenų apsaugos teisės doktrinos atstovų. D. Sancho teigia, kad BDAR 22 straipsnio 1 dalis yra suformuluota neigiamai, nes joje kalbama apie duomenų subjekto

teisę, kad jam „nebūtų taikomas <...> sprendimas“. Tai atitinka neigiamą duomenų valdytojo pareigą netaikyti išimtinai automatizuotų sprendimų (Sancho, 2020, p. 147). I. Mendoza L. ir A Bygrave teigimu, interpretuojant BDAR 22 straipsnio 1 dalį kaip bendrą draudimą, būtų geriau užtikrinamas BDAR tikslas – teisės į duomenų apsaugą užtikrinimas (Mendoza, Bygrave, 2017, p. 10). M. Brkan teigimu, sisteminis 22 straipsnio aiškinimas implikuoja, kad tik automatizuoti sprendimai, atitinkantys BDAR 22 straipsnio 2 dalies reikalavimus ir įtvirtinantys šio straipsnio 3 dalyje numatytas apsaugos priemones, yra leidžiami pagal BDAR (Brkan, 2018, p. 7) . Kai kurie autoriai[9] savo darbuose vadovaujasi požiūriu, kad BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas, plačiau šio straipsnio dviprasmiškumo klausimo nenagrinėdami.

Požiūrį, kad BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas taip pat patvirtina kol kas negausi BDAR 22 straipsnio taikymo praktika. Hagos apygardos teismas (oland. *Rechtbank Den Haag*) 2020 m. vasarį priimtame sprendime (Rechtbank Den Haag, 2020) ir Austrijos federalinis administracinis teismas (vok. *Bundesverwaltungsgericht*) 2020 m. gruodį priimtame sprendime (Bundesverwaltungsgericht, 2020) išreiškė poziciją, kad pagal BDAR 22 straipsnį yra taikomas bendras draudimas visiškai automatizuotai priimti individualius sprendimus, įskaitant profiliavimą, kurie turi teisinių pasekmių duomenų subjektui arba daro jam panašų reikšmingą poveikį. Atkreiptinas dėmesys, kad teismai neargumentavo, kodėl šiuo atveju duomenų subjekto teisė turi būti laikytina draudimu. ESTT klausimo, ar BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas tvarkyti duomenis šiame straipsnyje nurodytu būdu, ar duomenų subjekto teisė, nenagrinėjo.

Visgi, teisės doktrinos atstovų darbuose galima sutikti ir kitokių pozicijų. Anot S. Wachter et. al. galima teigti, kad egzistuoja BDAR 22 straipsnio 1 dalies dviprasmiškumas dėl panašių ES duomenų apsaugos direktyvos (BDAR pirmtakės) 15 straipsnio 1 dalies[10] ir BDAR 22 straipsnio 1 dalies formuluočių, kadangi nors ES duomenų apsaugos direktyva reguliavo automatizuotų sprendimų priėmimo klausimą iš esmės taip pat, tačiau ES valstybės narės šią nuostatą įgyvendino nevienodai, t. y. vienos šią nuostatą perkeldamos į nacionalinį reguliavimą pateikė ją kaip draudimą (pavyzdžiui, Vokietija), kitos – kaip teisę, reikalaujančią iš duomenų subjekto aktyvių veiksmų (pavyzdžiui, Jungtinė Karalystė) (Watcher et. al., 2017, p. 94–95).

[9] Pavyzdžiui, E. Falleti (Falleti, 2019, p. 6), F. A Rasso (Rasso, 2018, p. 6), B. Goodman ir S. Flaxman (Goodman ir Flaxman, 2017, p. 3).

[10] Valstybės narės suteikia kiekvienam asmeniui teisę, kad jo atžvilgiu nebus daromas sprendimas, kuris sukuria jam teisinį poveikį arba kuris ženkliai paveikia jį ir kuris yra paremtas tiktai automatiniu duomenų tvarkymu, skirtu įvertinti tam tikrus asmeniškus su juo susijusius aspektus, kaip antai: jo darbingumas, kreditingumas, patikimumas, elgesys ir kt. (ES duomenų apsaugos direktyvos 15 straipsnio 1 dalis).

L. Tosoni išsamiai analizuoja, kodėl BDAR 22 straipsnio 1 dalis turėtų būti suprantama kaip „teisė“, o ne kaip „draudimas“, toliau pateikiami keletas autoriaus argumentų:

Pirma, ES duomenų apsaugos direktyvos 15 straipsnio 1 dalies tekstu buvo siekiama įtvirtinti teisę, o ne draudimą. Iš esmės teisėkūros istorija[11] ir BDAR 22 straipsnio 1 dalies kilmė tvirtai nepagrindžia jos aiškinimo kaip bendro automatizuoto sprendimų priėmimo draudimo (Tosoni, 2021, p. 11).

Antra, L. Tosoni ginčija 29 straipsnio darbo grupės argumentus, kad BDAR preambulės 71 punktas patvirtina, jog BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas, kadangi preambulė neturi privalomos teisinės galios. Taip pat BDAR preambulės 71 punkte nėra aiškiai nurodyta, kad pagal BDAR 22 straipsnio 1 dalį įtvirtintas automatizuotas sprendimų priėmimas neturėtų būti leidžiamas (Tosoni, 2021, p. 14).

Trečia, BDAR 13 straipsnio 2 dalies f punkte, 14 straipsnio 2 dalies g punkte ir 15 straipsnio 1 dalies h punkte nustatyta, kad duomenų subjektai turi būti informuojami apie BDAR 22 straipsnio 1 dalyje nurodytą automatizuotą sprendimų priėmimą, įskaitant profiliavimą. Ši informavimo prievolė būtų absurdiška, jei pagal BDAR 22 straipsnio 1 dalį automatinis sprendimų priėmimas nebūtų leidžiamas, nes ją būtų galima suprasti kaip prievolę informuoti duomenų subjektus apie veiklą, kuri būtų draudžiama pagal BDAR (Tosoni, 2021, p. 17).

Ketvirta, L. Tosoni nesutinka su 29 straipsnio darbo grupės argumentu, kad aiškinant BDAR 22 straipsnio 1 dalį kaip teisę (ne kaip bendrą draudimą), BDAR 22 straipsnio 2 dalyje įtvirtintos išimtys nebūtų prasmingos. Autoriaus teigimu, jei BDAR 22 straipsnio 1 dalį aiškintume kaip teisę prieštarauti, pagrindinis skirtumas tarp naudojimosi teise pagal BDAR 22 straipsnio 1 dalį ir sutikimo išreiškimo pagal BDAR 22 straipsnio 2 dalies c punktą visų pirma yra susijęs laiko aspektu t. y. BDAR 22 straipsnio 1 dalyje

[11] ES duomenų apsaugos direktyvos 15 straipsnio 1 dalies ir atitinkamai BDAR 22 straipsnio 1 dalies ištakos siekia 1978 m. sausio 6 d. Prancūzijos įstatymo Nr. 78–17 dėl informacinių technologijų, duomenų rinkmenų ir pilietinių laisvių (pranc. *Loi Informatique et Liberté*). Šio įstatymo 2 straipsniu buvo draudžiama, kad teismininiai, administraciniai ir privatūs sprendimai, susiję su asmens elgesio vertinimu, būtų grindžiami automatizuotu asmens duomenų, skirtų tam tikriems jo asmenybės aspektams įvertinti, tvarkymu. Taigi šiame straipsnyje buvo nustatytas bendras draudimas priimti sprendimus, grindžiamus tik automatizuotu sprendimų priėmimu, kuriais vertinami asmenų asmeniniai aspektai. ES teisės aktų leidėjai, rengdami ES duomenų apsaugos direktyvos 15 straipsnio 1 dalį, rėmėsi pirmiau minėta Prancūzijos įstatymo nuostata, tačiau sąmoningai nusprendė bendrąjį draudimą paversti teise, kuria duomenų subjektai turi aktyviai naudotis. Tai buvo aiškiai paaiškinta abiejų nuostatų lyginamojoje analizėje, kurią Prancūzijos delegacija pateikė Tarybai per derybas dėl ES duomenų apsaugos direktyvos. Remiantis Prancūzijos delegacijos atlikta abiejų nuostatų analize: „Prancūzijos tekste nustatytas bendras draudimas, o direktyvos 15 straipsnio 1 dalyje atitinkamam asmeniui suteikiama teisė, kuria jis gali savo nuožiūra pasinaudoti. Priimant BDAR, ES teisės aktų leidėjai sąmoningai nepakeitė ES duomenų apsaugos direktyvos 15 straipsnio 1 dalies formuluotės, todėl ir BDAR 22 str. 1 d. nuostata turėtų būti suprantam kaip duomenų subjekto diskrecijoje esanti teisė, o ne bendras draudimas (Tosoni, 2021, p. 6–8).

numatyta teise paprastai ketinama naudotis *ex post*, t. y. po to, kai automatizuotas sprendimas jau priimtas <...> ir atvirkščiai, 22 straipsnio 2 dalies c punkte minimas sutikimas turėtų būti išreikštas *ex ante*, t. y. prieš priimant sprendimą, nes 22 straipsnio 2 dalies c punkte numatyta išimtis taikoma tik tuo atveju, jei sprendimas grindžiamas aiškiu duomenų subjekto sutikimu (Tosoni, 2021, p. 15).

Autoriaus nuomone, nors teisės nebūti automatizuotų sprendimų subjektu dviprasmiškumo problematikos diskurse dominuoja pozicija, kad BDAR 22 straipsnio 1 dalyje yra įtvirtintas bendras draudimas, visgi, šiai pozicijai oponuojančių autorių argumentai nėra nepagrįsti. Atsižvelgiant į tai, kategoriškos pozicijos užėmimas BDAR 22 straipsnio 1 dalies dviprasmiškumo klausimu neatrodo tikslingas. Turint omenyje vis dažnesnį DI technologijų taikymą praktikoje, atitinkamai ir BDAR 22 straipsnio 1 dalies taikymą tokių technologijų naudojimui, tik laiko klausimas kada ESTT, kaip, be kita ko, ES teisę aiškinantis organas, spręs šiame darbo skyriuje aptartą dviprasmiškumo problemą. ESTT išaiškinimas suteiktų teisinio aiškumo t. y. duomenų valdytojai tiksliai žinotų, kaip elgtis, kad nebūtų pažeisti šio straipsnio reikalavimai. Taip pat reikia pripažinti, kad šios teisės interpretavimo klausimas nėra vien tik teorinių ginčų objektas, kadangi skirtingos šios normos interpretacijos turėtų skirtingą praktinę įtaką duomenų valdytojams, priimantiems sprendimus, grindžiamus tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, kaip nurodyta BDAR 22 straipsnio 1 dalyje. Vienu atveju duomenų valdytojai apskritai negalėtų tvarkyti duomenų BDAR 22 straipsnio 1 dalyje nurodytu būdu (draudimo atvejis), nebent būtų remiamasi BDAR 22 straipsnio 2 dalyje įtvirtintomis išimtimis. Kitu atveju BDAR 22 straipsnio 1 dalyje nurodytu būdu tvarkyti duomenis būtų leidžiama, paliekant paskiriems asmenis teisę nesutikti su tokiu duomenų tvarkymu.

2.2. Teisės nebūti automatizuotai priimamų sprendimų subjektu taikymo sąlygos

BDAR 22 straipsnio 1 dalyje įtvirtinta, kad 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. Taigi, šios nuostatos taikymui turi būti tenkinamos šios kumuliatyvios sąlygos:
1) automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas turi būti taikomas duomenų subjektui, 2) sprendimas turi būti grindžiamas *tik* automatizuotu duomenų tvarkymu, įskaitant profiliavimą, 3) toks sprendimas turi sukelti teisines pasekmes arba daryti panašiu būdu daryti didelį poveikį. Šio darbo tikslais išvardintos sąlygos toliau bus nagrinėjamos kiekviena atskirai.

2.2.1. Tik automatizuotu duomenų tvarkymu grindžiamo sprendimo taikymo duomenų subjektui sąlyga

Kaip matyti iš BDAR 22 straipsnio 1 dalyje pateikiamo teisės apibrėžimo, tam, kad ši teisė būtų taikoma, automatizuotu duomenų tvarkymu grindžiamas sprendimas turi būti priimamas būtent duomenų subjekto atžvilgiu. Natūraliai kyla klausimas, kaip BDAR rėmuose turėtų būti suprantam duomenų subjekto sąvoka.

BDAR atskirai nepateikia duomenų subjekto sąvokos paaiškinimo, tačiau ją galima išvesti iš to, kaip BDAR apibrėžia asmens duomenis: bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas) (BDAR 4 straipsnio 1 punktas). Iš to seka, kad duomenų subjektas – fizinis asmuo, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti.

BDAR preambulės 14 punkte įtvirtinta, kad šiuo reglamentu užtikrinama apsauga turėtų būti taikoma fiziniams asmenims tvarkant jų asmens duomenis, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą. Šis reglamentas neapimama juridinių asmenų ir visų pirma su juridinio asmens statusą turinčių įmonių duomenų, įskaitant juridinio asmens pavadinimą, teisinę formą ir kontaktinius duomenis, tvarkymo.

BDAR preambulės 27 punkte įtvirtinta, kad šis reglamentas netaikomas mirusių asmenų asmens duomenims. Valstybės narės gali numatyti mirusių asmenų asmens duomenų tvarkymo taisykles. Taigi, BDAR suteikiama apsauga taikoma tik gyviems fiziniams asmenims, tačiau ne visiems, o tik tiems, kurių tapatybė nustatytą arba kurių tapatybę galima nustatyti.

Sprendžiant, ar galima nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visas priemones, pavyzdžiui, išskyrimą, kurias asmens tapatybei tiesiogiai ar netiesiogiai nustatyti, pagrįstai tikėtina, galėtų naudoti duomenų valdytojas ar kitas asmuo. Įsitikinant, ar tam tikros priemonės, pagrįstai tikėtina, galėtų būti naudojamos siekiant nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visus objektyvius veiksnius, pavyzdžiui, sąnaudas ir laiko trukmę, kurių prireiktų tapatybei nustatyti, turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą. Todėl duomenų apsaugos principai neturėtų būti taikomi anonimiškai informacijai, t. y. informacijai, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta (BDAR preambulės 26 punktas). Apskritai kalbant, galima laikyti, kad fizinio asmens tapatybė nustatyta, jeigu jis yra išskirtas iš visų kitų grupei priklausančių

asmenų. Panašiai fizinio asmens tapatybė gali būti nustatyta, t. y. ji dar nenustatyta, bet tai galima padaryti (Nuomonė 4/2007 dėl asmens duomenų sąvokos, 2007, p. 12).

Kaip matyti, BDAR saugo fizinius asmens net ir tais atvejais, kai nėra nustatyta asmens tapatybė, tačiau egzistuoja tik galimybė nustatyti šių fizinių asmenų tapatybę. ESTT byloje C–582/14 spręsdamas dėl to, ar to, kad duomenų valdytojas tvarko dinaminius IP adresus[12], pakanka, kad būtų galima konstatuoti, kad duomenų valdytojas turi galimybę nustatyti fizinio asmens tapatybę, pasakė, kad elektroninių paslaugų teikėjas (duomenų valdytojas) gali pasinaudoti tam tikromis priemonėmis, kad padedamas kitų subjektų, t. y. kompetentingos institucijos ir interneto prieigos teikėjo, nustatytų atitinkamo asmens tapatybę pagal išsaugotus IP adresus (Patrick Breyer v. Bundesrepublik Deutschland, 2016). Kitais žodžiais tariant, jei duomenų valdytojas, tvarkydamas tik dinaminį IP adresą pats negali tiesiogiai nustatyti fizinio asmens tapatybės, tačiau turi teorinę galimybę pasikreipus į kitus subjektus ir iš jų gavus papildomą informaciją išskirti konkretų fizinį asmenį, turėtų būti laikoma kad duomenų valdytojas turi galimybę nustatyti fizinio asmens tapatybę ir dėl to, dinaminis IP adresas turėtų būti laikomas asmens duomeniu ir tokiam fiziniam asmeniui turi būti taikoma BDAR suteikiama apsauga.

Pažymėtina, kad fiziniams asmenims yra taikoma BDAR suteikiama apsauga tik tais atvejais, kai yra tvarkomi jų asmens duomenys t. y. duomenys, pagal kuriuos yra nustatyta, arba gali būti nustatyta fizinio asmens tapatybė. Atitinkamai ir BDAR 22 straipsnio 1 dalis taikoma tik tais atvejais, kai yra tvarkomi ne duomenys plačiąja prasme, bet būtent asmens duomenys.

Taigi, tam, kad būtų išpildyti šiame darbo poskyryje aptariama sąlyga, reikalinga, kad tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas būtų priimtas gyvo fizinio asmens, kurio tapatybė nustatyta arba kurio tapatybę teoriškai galima nustatyti, atžvilgiu.

[12] Kiekvienas prie interneto jungiamas kompiuteris turi savo IP adresą – tam tikrą skaičių seką, priskiriamą konkrečiam kompiuteriui. Dinaminiai IP adresai yra laikini, suteikiami kiekvieną kartą prisijungus prie interneto ir keičiami per vėlesnius prisijungimus, o ne „statiniai“ IP adresai, kurie nekinta ir leidžia ilgam laikui identifikuoti prie tinklo prijungtą įrenginį.

2.2.2. Tik automatizuotu duomenų tvarkymu grindžiamas sprendimas

Kaip matyti iš BDAR 22 straipsnio 1 dalies, duomenų subjektas turi teisę, kad jam nebūtų taikomas *tik* automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas t. y. BDAR 22 straipsnis yra taikomas tik tais atvejais, kai viso sprendimo priėmimo proceso metu nedalyvauja žmogus. Atitinkamai, jeigu žmogus sprendimo priėmimo procese dalyvauja, BDAR 22 straipsnyje įtvirtinta teisė nėra taikoma, todėl svarbu išsiaiškinti ką būtent reiškia žmogaus (ne)dalyvavimas sprendimo priėmimo procese.

Duomenų valdytojas negali imituoti žmogaus įsikišimo ir taip išvengti 22 straipsnio nuostatų. Kad būtų pripažinta, jog esama žmogaus įsikišimo. duomenų valdytojas privalo užtikrinti, kad bet koks sprendimo peržiūrėjimas būtų prasmingas, o ne apsimestinis veiksmas. Sprendimą turėtų peržiūrėti asmuo, kuriam yra suteikti įgaliojimai pakeisti sprendimą ir kuris yra kompetentingas tai padaryti. Atlikdamas analizę, tas asmuo turėtų atsižvelgti į visus susijusius duomenis (29 straipsnio darbo grupės gairės, 2018, p. 22). Logiškai seka, kad duomenų valdytojams siekiant integruoti į sprendimo priėmimą žmogų (tokiu būdu išvengiant BDAR 22 straipsnio taikymo), reikalinga, kad žmogus gebėtų pilnai suprasti priimamo sprendimo logiką, sugebėtų išanalizuoti visus duomenis, reikalingus sprendimui priimti. Jeigu faktiškai žmogus sprendimo priėmimo procese dalyvauja tik fiktyviai, tuomet vis vien būtų laikoma, kad sprendimas yra priimtas remiantis tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą. Pavyzdžiui, taikant automatizuotą procesą parengiama tam tikra rekomendacija dėl duomenų subjekto. Jei, priimant galutinį sprendimą, koks nors žmogus peržiūri kitus veiksnius ir į juos atsižvelgia, toks sprendimas nebus pagrįstas tik automatizuotu duomenų tvarkymu (29 straipsnio darbo grupės gairės, 2018, p. 22). Remiantis šiuo pavyzdžiu, jeigu taikant automatizuotą procesą parengiama rekomendacija dėl duomenų subjekto, bet priimant galutinį sprendimą žmogus tik patvirtinta rekomendaciją ir realaus poveikio sprendimui nedaro, tuomet bus laikoma, kad toks sprendimas yra pagrįstas tik automatizuotu duomenų tvarkymu.

Taigi, tam, kad būtų tenkinama tik automatizuotu duomenų tvarkymų grindžiamo sprendimo sąlyga, sprendimas turi būti priimamas be žmogaus realaus (galinčio iš esmės daryti įtaką priimamam sprendimui) įsikišimo.

2.2.3. Teisinių pasekmių arba kitokio panašaus poveikio sąlyga

BDAR 22 straipsnio 1 dalis taikoma tik tais atvejais, kai dėl tokio sprendimo duomenų subjektui kyla teisinės pasekmės, arba toks sprendimas jam panašiu būdu daro kitokį didelį poveikį. Nors BDAR nėra įtvirtinta, ką reiškia „kyla teisinės pasekmės“ arba „panašiu būdu daro kitokį didelį poveikį“, tačiau, anot 29 straipsnio darbo grupės, iš formuluotės aišku, kad kalbama tik apie rimtas ir dideles pasekmes (29 straipsnio darbo grupės gairės, 2018, p. 22).

Kad kiltų teisinių pasekmių, tik automatizuotu duomenų tvarkymu pagrįstas sprendimas turi turėti įtakos kokio nors asmens juridinėms teisėms, pavyzdžiui, asociacijų laisvei, balsavimo teisei arba teisei imtis teisinių veiksmų. Teisinė pasekmė taip pat gali būti susijusi su poveikiu asmens juridiniam statusui arba teisėms, kurios jam buvo suteiktos kokia nors sutartimi. Tokio poveikio pavyzdžiai: su asmeniu susiję automatizuoti sprendimai, dėl kurių nutraukiama sutartis, suteikiama arba nesuteikiama tam tikra įstatymu numatyta socialinė išmoka, pavyzdžiui, išmoka vaikui išlaikyti arba būsto išlaidoms padengti, atsisakoma įleisti į šalį arba suteikti pilietybę (29 straipsnio darbo grupės gairės, 2018, p. 22).

Visgi, net jei nepasikeičia duomenų subjekto juridines teisės arba pareigos, jam vis tiek gali būti padarytas pakankamai didelis poveikis, dėl to būtų taikomas BDAR 22 straipsnio 1 dalis. Formuluotė „panašiu būdu“ implikuoja, kad riba, kuri turi būti pasiekta, kad sprendimo poveikis būtų didelis, turi būti panaši į sprendimo, dėl kurio kyla teisinių pasekmių (29 straipsnio darbo grupės gairės, 2018, p. 22). BDAR preambulės 71 punkte pateikiami tokie pavyzdžiai, kuomet sprendimas darytų kitokį panašų didelį poveikį: automatinio internetinės kredito paraiškos atmetimas ar elektroninio įdarbinimo praktika be žmogaus įsikišimo. 29 straipsnio darbo grupė papildomai pateikia tokius pavyzdžius, kuomet galėtų būti laikoma, kad sprendimas padarė didelį poveikį: 1) buvo paveiktos kokio nors asmens finansinės aplinkybės, pvz., galimybė gauti kreditą, 2) buvo paveiktos asmens galimybės gauti sveikatos priežiūros paslaugas, 3) buvo paveikta asmens galimybė gauti išsilavinimą (pvz. įstoti į universitetą), 4) buvo paveikta asmens galimybė įsidarbinti (29 straipsnio darbo grupės gairės, 2018, p. 22–23). Nėra baigtinio sąrašo automatizuotų sprendimų, kurie galėtų daryti asmeniui kitokį panašų didelį poveikį ir tai, ar poveikis yra didelis, ar ne, yra vertinamasis kriterijus, todėl darytina išvada, kad BDAR 22 straipsnio taikymo apimtis, toje dalyje, kiek konkrečiu atveju bus reikalinga nuspręsti, ar automatizuotas sprendimas padarė „kitokį panašų didelį poveikį“, priklausys nuo to, kaip plačiai priežiūros institucijos ir teismai aiškins sąvoką „kitoks panašus didelis poveikis“.

Tai svarbu, kadangi nuo šio kriterijaus aiškinimo apimties priklausys ir BDAR 22 straipsnio 1 dalyje įtvirtintos teisės taikymo apimtis.

Apibendrinant šio darbo 2.2 skyrių, darytina išvada, kad duomenų valdytojams, savo veikloje pasitelkiantiems DI, BDAR 22 straipsnis bus taikomas tais atvejais, kai: 1) DI atliekamas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas bus nukreiptas į duomenų subjektą, 2) toks DI sprendimas duomenų subjektui sukels teisines pasekmes ar kitokiu panašiu būdu darys didelį poveikį ir 3) DI veiks be žmogaus realaus įsikišimo.

2.3. Teisės nebūti automatizuotai priimamų sprendimų subjektu taikymo ribos

Kaip minėta, BDAR 22 straipsnio 1 dalyje yra įtvirtinta duomenų subjektų teisė nebūti automatizuotai priimamų sprendimų subjektu. Visgi, šio straipsnio 2 dalyje įtvirtinta, kad 22 straipsnio 1 dalis nėra taikoma, kuomet automatizuotu duomenų tvarkymu grindžiamas sprendimas, įskaitant profiliavimą: a) yra būtinas siekiant sudaryti arba vykdyti sutartį tarp duomenų subjekto ir duomenų valdytojo, arba b) yra leidžiamas Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui ir kuri taip pat nustato tinkamas priemones duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti; arba c) yra pagrįstas aiškiu duomenų subjekto sutikimu.

Taigi, galima teigti, kad BDAR 22 straipsnio 2 dalyje įtvirtintos išimtys nubrėžia BDAR 22 straipsnio 1 dalyje įtvirtintos teisės ribas. M. Brkan, analizuodama šias išimtis, teigė, kad nors BDAR 22 straipsnio 1 dalyje yra nustatyta teisė duomenų subjektams, kad jų atžvilgiu nebūtų priimti tik automatizuotu duomenų tvarkymu grindžiami sprendimai, įskaitant profiliavimą, tačiau šios teisės išimtys šią teisę susiaurina tiek, kad pačios išimtys tampa taisykle (Brkan, 2018, p. 24). Jeigu sutiktume su M. Brkan išreikšta pozicija, turėtume pripažinti, kad teisė nebūti automatizuotų sprendimų subjektu yra taikoma tik išimtiniais atvejais. Toliau BDAR 22 straipsnio 2 dalies išimtys bus nagrinėjamos kiekviena atskirai, siekiant įvertinti, ar iš tikrųjų duomenų valdytojams yra taip paprasta remiantis išimtimis išvengti BDAR 22 straipsnio 1 dalies taikymo.

2.3.1. Sutarties išimtis

BDAR 22 straipsnio 2 dalies a punktas teigia, kad 22 straipsnio 1 dalis nėra taikoma, kai sprendimas yra būtinas siekiant sudaryti arba vykdyti sutartį tarp duomenų subjekto ir

duomenų valdytojo. Duomenų valdytojas ir duomenų subjektas turi būti automatizuotą sprendimų priėmimą pateisinančios sutarties šalimis. Tokia sutartis gali būti jau sudaryta arba dar ketinama sudaryti. Sutarties pobūdis neturi reikšmės. Pavyzdžiui, duomenų valdytojas galėtų priimti tik automatizuotu duomenų tvarkymu grindžiamą sprendimą dėl to, ar gali su asmeniu sudaryti darbo sutartį arba ar klientas toliau gali vykdyti finansinių paslaugų sutartį (Zaleskis, 2018, p. 215). Duomenų valdytojo galimybė pateisinti tik automatizuotu duomenų tvarkymu grindžiamą sprendimą priklausytų iš esmės nuo to, ar toks duomenų tvarkymas yra „būtinas“ sutarčiai sudaryti ar vykdyti, todėl „būtinumo“ kriterijus bus nagrinėjamas plačiau.

ESTT byloje C–524/06 teigė, kad „būtinumas“ yra autonomiška Bendrijos sąvoka, kurią reikia aiškinti taip, kad ji visiškai atitiktų Direktyvos 95/46/EB [*ES duomenų apsaugos direktyvos – aut past.*] tikslą įtvirtintą jos 1 straipsnio 1 dalyje [*privatumo teisės tvarkant asmens duomenis apsaugą – aut. past.*] (Heinz Huber v Bundesrepublik Deutschland, 2008). Taigi, analogiškai būtinumo sąvoka BDAR kontekste turi būti nagrinėjama atsižvelgiant į BDAR 1 straipsnio 2 dalyje įtvirtintą tikslą –fizinių asmenų pagrindinių teisių ir laisvių apsaugą (visų pirma jų teisę į duomenų apsaugą).

Anot 29 straipsnio darbo grupės būtinumas sudaryti ar vykdyti sutartį su duomenų subjektu turi būti aiškinamas griežtai (siaurai) ir jis neapima atvejų, kai duomenų tvarkymas nėra iš tikrųjų būtinas sutarčiai vykdyti, o duomenų valdytojas jį vienašališkai primeta duomenų subjektui. Be to, tai, kad tam tikras duomenų tvarkymas yra numatytas sutartyje, savaime nereiškia, kad duomenų tvarkymas yra būtinas sutarčiai vykdyti. Net jei duomenų tvarkymo veiksmai yra konkrečiai paminėti <...> sutartyje, vien dėl šio fakto jie nėra "būtini" sutarčiai vykdyti (Article 29 Working Party Opinion, 2014, p. 16–17). Tokį požiūrį patvirtina ir ESTT praktika. Byloje C–13/16 ESTT pažymėjo, kad dėl sąlygos, susijusios su būtinybe tvarkyti duomenis, primintina, kad nukrypimai nuo asmens duomenų apsaugos ir jos apribojimai neturi viršyti to, kas griežtai būtina (Rigas satiksme, 2017).

Duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi BDAR principų, ir turi sugebėti įrodyti, kad jų laikomasi (atskaitomybės principas) (BDAR 5 straipsnio 1 dalis), todėl svarbu aiškinti šią sąvoka sistemoje su BDAR 5 straipsnyje įtvirtintais principais. Aiškinant būtinumo sąvoką ypač didelę reikšmę turi duomenų kiekio mažinimo principas, kuris sako, kad asmens duomenys turi būti adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi (BDAR 5 straipsnio 1 dalies c punktas), todėl duomenų valdytojams kyla pareiga įvertinti, ar tvarkyti asmens duomenys iš tiesų yra būtina, siekiant sudaryti ar vykdyti sutartį. Anot 29 straipsnio darbo grupės, tarp duomenų tvarkymo ir sutarties vykdymo tikslo turi būti tiesioginis ir objektyvus ryšys (29 straipsnio

darbo grupės gairės, 2017, p. 9). „Būtinumo“ sąvokos nereikėtų tapatinti su „naudos“ sąvoka, kadangi, kaip teigia EDAV, duomenų tvarkymas turi būti objektyviai būtinas sutarčiai sudaryti ar vykdyti t. y. negalima remtis tik tuo, kad atitinkamas duomenų tvarkymas yra duomenų valdytojui naudingas verslo procesuose (EDPB Guidelines 2/2019, 2019, p. 8).

Taigi, tik sisteminis BDAR nuostatų interpretavimas ir taikymas gali padėti atsakyti, ar konkrečiu atveju duomenis tvarkyti yra būtina. Kaip teigia M. Brkan, jei BDAR 22 straipsnio 2 dalies a punkto prasmę reikėtų aiškinti labai griežtai, abejotina, ar ji kada nors atvertų kelią automatizuotiems sprendimams. Pavyzdžiui, galima teigti, kad sudarant draudimo ar paskolos sutartį būtina įvertinti riziką, tačiau ar ši rizika būtinai turi būti vertinama automatizuotomis priemonėmis? (Brkan, 2018, p. 11). Kaip minėta, tiek 29 straipsnio darbo grupė, tiek ESTT „būtinumo“ sąvoka aiškina siaurai, todėl ir duomenų valdytojai, siekiantys pagrįsti tik automatizuotu būdu priimamus sprendimus BDAR 22 straipsnio 2 dalies a punkte įtvirtinta išimtimi, turėtų į tai atsižvelgti.

Pavyzdžiui, duomenų valdytojas, vykdydamas darbuotojų atranką, pasitelkia DI technologijas tam, kad jos, remiantis surinktais asmens duomenimis apie kandidatus (amžius, lytis, gyvenimo aprašymas ir t. t.) tik automatizuotu būdu priimtų sprendimą dėl to, ar priimti asmenį į darbą, ar ne. Įsivaizduokime dvi skirtingas situacijas, kai: a) duomenų valdytojas A yra sąlyginai mažai žinoma įmonė, į kurios skelbiamą laisvą darbo vietą pretenduoja 10 kandidatų, ir b) duomenų valdytojas B yra žinoma įmonė, į kurios laisvą darbo vietą pretenduoja 200 kandidatų. Tokioje situacijoje akivaizdu, kad duomenų valdytojui A būtų sunku pagrįsti, kodėl šioje situacijoje yra būtina sprendimą grįsti tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą ir atsakyti į klausimą, ar negalima to paties tikslo (kandidatų atrankos) vykdyti mažiau duomenų subjektų teises ir interesus ribojančiomis priemonėmis. Priešingai, duomenų valdytojas B galėtų argumentuoti, kad toks tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas yra būtinas siekiant vykdyti kandidatų į darbo vietas atranką, kadangi dėl didelio kandidatų skaičiaus paraiškų peržiūra kitais būdais (pvz. atranką vykdant žmogui) pareikalautų neproporcingų išteklių.

Galima apibendrinti, kad duomenų valdytojai sutarties išimtimi gali remtis tik ribotais atvejais. Duomenų valdytojas turi sugebėti įrodyti, kodėl yra būtina priimti BDAR 22 straipsnio 1 dalyje nurodytus sprendimus siekiant sudaryti ar vykdyti sutartį su duomenų subjektu.

EDAV teigimu tais atvejais, kai duomenų tvarkymas iš tikrųjų nėra būtinas sutarčiai įvykdyti, toks duomenų tvarkymas gali būti atliekamas tik tuo atveju, jei jis grindžiamas

kitu tinkamu teisiniu pagrindu (EDPB Guidelines 2/2019, 2019, p. 7), todėl toliau bus aptariamos kitos alternatyvios išimtys, kuriomis duomenų valdytojai gali remtis priimant tik automatizuotu asmens duomenų tvarkymu, įskaitant profiliavimą, grindžiamus sprendimus.

2.3.2. ES ar valstybės narės teisės išimtis

BDAR 22 straipsnio 2 dalies b punkte įtvirtinta, kad BDAR 22 straipsnio 1 dalis nėra taikoma, kai sprendimas yra leidžiamas Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui ir kuria taip pat nustatomos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti.

BDAR preambulės 71 punkte teigiama, kad tokiu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimų priėmimas turėtų būti leidžiamas, kai jis yra aiškiai leidžiamas Sąjungos ar valstybės narės teisėje, kuri taikoma duomenų valdytojui, be kita ko, sukčiavimo ir mokesčių slėpimo stebėsenos ir prevencijos tikslais, laikantis Sąjungos institucijų ar nacionalinių priežiūros įstaigų taisyklių, standartų ir rekomendacijų, ir siekiant užtikrinti duomenų valdytojo suteiktos paslaugos saugumą ir patikimumą.

BDAR 22 straipsnio 2 dalies b punkte nėra nurodytos konkrečios duomenų subjektų teisių ir interesų apsaugos priemonės (priešingai nei BDAR 22 straipsnio 3 dalyje[13]). Kaip teigia L. A. Bygrave, šiuo atžvilgiu valstybėms narėms suteikta gana plati diskrecija, ypač dėl to, kad „tinkamos priemonės“, reikalingos duomenų subjektų apsaugai užtikrinti, nurodytos gana bendrai (angl. *specified in relatively general terms*) (Bygrave, 2020, p. 537).

Iš viešai prieinamos informacijos galima daryti išvadą, kad tiek ES, tiek Lietuvos lygmeniu nėra priimta teisės aktų, kurie leistų BDAR 22 straipsnio 1 dalyje apibrėžtą sprendimų priėmimą. Autoriaus nuomone, BDAR 22 straipsnio 2 dalies b punkte numatyta išimtis galėtų būti priemone, kuria ES valstybės narės galėtų pasinaudoti siekiant atverti platesnes galimybes duomenų valdytojams naudoti DI technologijas, tuo pačiu teisės aktuose numatant tinkamas duomenų subjektų teisių ir interesų apsaugos priemones, kurias būtų galima diferencijuoti atsižvelgiant į pavojus, kuriuos kelia teisės aktu leidžiamas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas. Be to pačiu, automatizuotų sprendimų priėmimo reguliavimas teisės aktais suteiktų duomenų

[13] BDAR 22 str. 3 d. nurodytos priemonės apima, bent jau teisę iš duomenų valdytojo reikalauti žmogaus įsikišimo, pareikšti savo požiūrį ir užginčyti sprendimą.

valdytojams teisinį aiškumą – būtų paprasta nustatyti, koks duomenų tvarkymas yra leidžiamas ir kokias tinkamas duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemones reikalinga įgyvendinti siekiant nepažeisti teisės akto.

2.3.3. Sutikimo išimtis

BDAR 22 straipsnio 2 dalies c punktas teigia, kad 22 straipsnio 1 dalis nėra taikoma, kai sprendimas yra pagrįstas aiškiu duomenų subjekto sutikimu. Visų pirma tikslinga pateikti 29 straipsnio darbo grupės požiūrį dėl standarto, kuris turi būti keliamas iš duomenų subjekto gaunamam sutikimui: asmens sprendimui sutikti su duomenų tvarkymu turėtų būti taikomi griežti reikalavimai, ypač atsižvelgiant į tai, kad tai darydamas asmuo gali atsisakyti pagrindinės teisės (angl. *waiving a fundamental right*) (Opinion 15/2011 on the definition of consent, 2011, p. 8).

Pažymėtina, kad sutikimas turi būti „aiškus“ (ang. *explicit*) t. y. taikomas toks pat standartas, koks nustatytas specialių kategorijų asmens duomenų tvarkymui pagal BDAR 9 straipsnio 2 dalies a punktą (Bygrave, 2020, p. 537). Aiškus sutikimas yra reikalingas tam tikromis aplinkybėmis, kai kyla rimta su duomenų apsauga susijusi rizika, todėl manoma, kad reikia griežtos individualios asmens duomenų kontrolės. Terminas „aiškus“ reiškia tai, kaip duomenų subjektas išreiškia sutikimą (Gairės 05/2020 dėl sutikimo, 2020, p. 21). Taigi, duomenų valdytojams, kurie remiasi BDAR 22 straipsnio 2 dalies c punkte įtvirtinta išimtimi, remiantis atskaitomybės principu (BDAR 5 str. 2 d.), kyla pareiga įrodyti, kad duomenų subjektas sutikimą dėl duomenų tvarkymo išreiškė aiškiu būdu. Iš esmės tai reiškia, kad duomenų valdytojai turi turėti įrodymus (pvz. raštiškus, garsinius) dėl to, kad duomenų subjektas davė sutikimą.

BDAR 4 straipsnio 11 punkte sutikimas yra apibrėžiamas kaip 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 42 konstatuojamosios dalies punkte teigiama, kad sutikimas neturėtų būti laikomas duotas laisva valia, jei duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti, nepatirdamas žalos. Tai reiškia, kad dėl duomenų subjekto atsisakymo duoti sutikimą duomenų valdytojai negali, pavyzdžiui, atsisakyti suteikti paslaugą. Apskritai kalbant, sutikimas yra negaliojantis, kai duomenų subjektui daromas bet koks netinkamas spaudimas ar įtaka (kurių išraiška gali būti labai

įvairi) ir duomenų subjektas dėl to negali naudotis savo laisva valia (29 straipsnio darbo grupės gairės, 2017, p. 6).

Duomenų valdytojams, naudojantiems DI technologijas savo veikloje tai reikštų, kad jie negalėtų atsisakyti suteikti duomenų subjektui savo paslaugų, net jei duomenų subjektas neduotų sutikimo jo atžvilgiu priimti tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamų sprendimų. Tokiu atveju duomenų valdytojams, siekiantiems pagrįsti BDAR 22 straipsnio 1 dalyje atliekamą duomenų tvarkymą sutikimo išimtimi, lieka vienintelė alternatyva – jeigu duomenų subjektas neduoda sutikimo, turi būti užtikrinta, kad duomenų subjektas vis tiek gaus paslaugas ir be tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamų sprendimų priėmimo. Praktikoje duomenų valdytojams naudojantiems DI technologijas tai gali kelti iššūkių, kadangi 1) užtikrinti alternatyvų procesą (be BDAR 22 straipsnio 1 dalyje apibrėžtų sprendimų priėmimo) gali kainuoti neproporcingai daug išteklių, arba b) dėl DI technologijų pranašumo prieš žmogų (efektyvumas, gebėjimas apdoroti didelius duomenų kiekius kt.), tam tikrais atvejais suteikti paslaugas nebūtų įmanoma. Jeigu nėra užtikrinama, kad asmeniui atsisakius duoti sutikimą, jam vis tiek būtų suteiktos paslaugos, duomenų valdytojas BDAR 22 straipsnio 2 dalies c punkte įtvirtinta išimtimi neturėtų.

BDAR 43 konstatuojamosios dalies punkte teigiama, kad sutikimas neturėtų būti laikomas pagrįstu asmens duomenų tvarkymo teisiniu pagrindu konkrečiu atveju, kai yra aiškus duomenų subjekto ir duomenų valdytojo padėties disbalansas. Būtent toks disbalansas egzistuoja darbovietėje tarp darbdavio ir darbuotojų. Remiantis EDPB išaiškinimu, dėl darbdavio ir darbuotojo santykiams būdingos priklausomybės nėra tikėtina, kad duomenų subjektas galėtų neduoti savo darbdaviui sutikimo, kad butų tvarkomi jo duomenys, be baimes ar realios rizikos patirti neigiamą poveikį dėl savo nesutikimo <...>, todėl 29 straipsnio darbo grupė mano, kad darbdavių rėmimasis sutikimu, tvarkant savo dabartinių ar busimų darbuotojų asmens duomenis, yra problemiškas, nes nėra tikėtina, kad toks sutikimas butų duotas laisva valia (Guidelines 05/2020 on consent, 2020, p. 9). Taigi, remtis sutikimo pagrindu tvarkant darbuotojų duomenis iš esmės galima tik išimtiniais atvejais, kai iš tiesų galima įrodyti, kad darbuotojai nepatirtų jokių neigiamų pasekmių dėl atsisakymo duoti sutikimą. Toks pat aiškinimas turėtų būti taikomas ir kitais atvejais, kai tarp duomenų subjekto ir duomenų valdytojo yra padėties (galios) disbalansas, pavyzdžiui, kai duomenų valdytojas yra valstybė.

Reikalavimu, kad sutikimas būtų „konkretus“, siekiama duomenų subjektui užtikrinti tam tikrą vartotojo turimą kontrolę ir skaidrumą. Jei duomenų valdytojas remiasi duomenų subjekto sutikimu, duomenų subjektai visada turi duoti sutikimą dėl konkretaus

duomenų tvarkymo tikslo (29 straipsnio darbo grupės gairės, 2017, p. 12). Toks aiškinimas grindžiamas, *inter alia*, BDAR 5 straipsnio 1 dalies b punkte įtvirtintu tikslo apribojimo principu, kurio esmę sudaro nuostata, kad asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu. Tai reiškia, kad duomenų valdytojas turi gauti asmens sutikimą dėl konkretaus duomenų tvarkymo tikslo ir negali tvarkyti to asmens duomenų vėliau kitais (nesuderinamais) tikslais, dėl kurių nėra gautas sutikimas[14]. Vienas iš DI technologijų[15] privalumų yra gebėjimas mokytis ir prieiti iš anksto nenumatytų išvadų, tuo pačiu sugeneruojant „naujus“ asmens duomenis. DI naudojantiems duomenų valdytojams gali kilti poreikis panaudoti tokius asmens duomenis ir naujiems (iš anksto nenumatytiems) tikslams. Pavyzdžiui, mygtuko „patinka“ paspaudimai iš esmės skirti asmens nuomonei tam tikru klausimu išreikšti, tačiau ar gali tokie duomenys būti toliau naudojami siekiant daryti tam tikras išvadas apie asmens psichologinę būklę, komercinius polinkius, politines pažiūras?[16] Anot 29 straipsnio darbo grupės, tokiais atvejais reikia įvertinti keletą svarbių veiksnių, įskaitant, be kita ko, ryšį tarp pradinio tikslo ir tolesnio duomenų tvarkymo tikslo bei kontekstą, kuriame duomenys buvo surinkti. Iš esmės kuo didesnis atstumas tarp pradinio tikslo, nurodyto renkant duomenis, ir tolesnio naudojimo tikslų, tuo išsamesnė ir visapusiškesnė turės būti analizė, be to, gali reikėti įvertinti daug papildomų kriterijų. Tokiais atvejais taip pat gali prireikti įtraukti papildomas apsaugos priemones, kad būtų kompensuotas tikslo pasikeitimas (pavyzdžiui, duomenų subjektui suteikti papildomos informacijos ir aiškią pasirinkimo galimybę nesutikti) (Opinion 03/2013 on purpose limitation, 2013, p. 22).

Duomenų subjektas turi suprasti dėl ko jis duoda sutikimą. Kaip teigia 29 straipsnio darbo grupė, bet kokiu atveju duomenų subjektai turėtų turėti pakankamai atitinkamos informacijos apie numatomą duomenų tvarkymo naudojimą ir pasekmes, kad būtų užtikrinta, jog bet koks jų duodamas sutikimas būtų pagrįstas informacija. Kodėl duomenų valdytojams gali būti sudėtinga suteikti duomenų subjektams pakankamai informacijos, susijusios su jų atžvilgiu priimamų automatizuotų sprendimų priėmimu, plačiau nagrinėjama šio darbo 3.3 skyriuje.

[14] Pavyzdžiui, asmeniui sutikus, kad jo duomenys būtų tvarkomi prekės pristatymo tikslu, negalima naudoti to asmens duomenų skambinant asmeniui rinkodaros tikslais.

[15] Šiuo atveju kalbama apie tokias DI rūšis, kurios naudoja įvesties duomenis naujoms išvesties reikšmėms prognozuoti (pvz. mašininis mokymasis, gilusis mokymasis) t. y. ne tik atlieka „paprastas“ algoritmines funkcijas, tačiau tuo pačiu gali mokytis ir pateikti naujų (iš anksto nenumatytų) išvadų.

[16] 2013 m. atlikto tyrimo metu nustatyta, kad remiantis *Facebook* mygtuko „patinka“ paspaudimais, tyrimo metu naudotas modelis teisingai atskyrė homoseksualius ir heteroseksualius vyrus 88 % atvejų, afroamerikiečius ir baltaodžius amerikiečius 95 % atvejų ir demokratus bei respublikonus 85 % atvejų (Kosinski et. al. 2013).

Apibendrinant, duomenų valdytojams, naudojantiems DI technologijas ir siekiantiems pagrįsti BDAR 22 straipsnio 1 dalyje nurodytą sprendimų priėmimą aiškaus sutikimo išimtimi gali kilti sunkumų, kadangi 1) atsižvelgiant į sutikimui keliamą „laisvos valios“ reikalavimą, užtikrinti, kad duomenų subjektui atsisakant duoti sutikimą dėl jo duomenų tvarkymo, duomenų subjektas dėl savo nesutikimo nepatirtų žalos, praktiškai gali pareikalauti neproporcingai daug išteklių arba apskritai būti neįmanoma, 2) remtis sutikimo išimtimi, kai tarp duomenų valdytojo ir duomenų subjekto egzistuoja padėties (galios) disbalansas, pavyzdžiui, darbovietėje galima tik išimtiniais atvejais, 3) sudėtinga tiksliai nurodyti duomenų tvarkymo tikslus, dėl kurių prašoma sutikimo tais atvejais, kai duomenų valdytojas naudoja DI technologijas, galinčias generuoti naujas išvadas (mokytis) ir dėl ko gali kilti poreikis tvarkyti duomenis naujais tikslais.

Apibendrinant šio darbo 2.3 skyrių, darytina išvada, kad nėra pakankamo pagrindo sutikti su M. Brkan išreikšta pozicija, kad BDAR 22 straipsnio 2 dalyje įtvirtintos išimtys susiaurina BDAR 22 straipsnio 1 dalyje įtvirtintą teisę tiek, kad pačios išimtys tampa taisykle. Priešingai, įvairios sąlygos, kurias duomenų valdytojai turi išpildyti, norėdami pasinaudoti BDAR 22 straipsnio 2 dalyje įtvirtintomis išimtimis, ypač DI naudojimo kontekste, apsunkina duomenų valdytojams galimybę remtis šiomis išimtimis priimant tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamus sprendimus. Visgi, BDAR 22 straipsnio 2 dalies b punktas įtvirtina plačią diskreciją ES valstybių narių įstatymų leidėjams „įteisinti“ BDAR 22 straipsnio 1 dalyje aprašytus automatizuotus sprendimus nacionaliniu lygmeniu. Tai prisidėtų prie DI technologijų kūrimo ir naudojimo skatinimo bei įneštų teisinio aiškumo – duomenų valdytojai, naudojantys DI technologijas, galėtų būti užtikrinti dėl savo veiklos teisėtumo bei tiksliai žinotų, kokias tinkamas duomenų subjektų teisių ir interesų apsaugos priemones jiems reikia įgyvendinti.

2.4. Automatizuotų sprendimų priėmimas tvarkant specialiųjų kategorijų asmens duomenis

BDAR 22 straipsnio 4 dalyje įtvirtinta, kad 2 dalyje nurodyti sprendimai negrindžiami 9 straipsnio 1 dalyje nurodytais specialių kategorijų asmens duomenimis, nebent taikomi 9 straipsnio 2 dalies a arba g punktai ir yra nustatytos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti. Ši nuostata iš esmės reiškia, kad kai yra tvarkomi specialiųjų kategorijų asmens duomenys, tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, priimami sprendimai yra draudžiami, nebent jie:

- būtų grindžiami BDAR 9 straipsnio 2 dalies a[17] arba g[18] punktais ir
- būtų nustatytos tinkamos priemonės duomenų subjekto teisėms bei laisvėms ir teisėtiems interesams apsaugoti.

BDAR 22 straipsnio 4 dalyje nėra minimos konkrečios duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonės, todėl šiuo atveju ES teisės aktų leidėjas paliko plačią diskreciją duomenų valdytojams patiems nustatyti, atsižvelgiant į atskaitomybės principą (BDAR 5 straipsnio 2 dalis), kokias konkrečias priemones įgyvendinti. Visgi, atsižvelgiant į tai, kad specialiųjų kategorijų duomenų tvarkymas kelia didesnes rizikas duomenų subjektams, priemonės, skirtos apsaugoti duomenų subjektus, turėtų apimti bent jau priemones, nurodytas BDAR 22 straipsnio 3 dalyje, kurių problematika DI kontekste plačiau analizuojama šio darbo 3.1 skyriuje.

[17] Duomenų subjektas aiškiai sutiko, kad tokie asmens duomenys būtų tvarkomi vienu ar keliais nurodytais tikslais, išskyrus atvejus, kai Sąjungos arba valstybės narės teisėje numatyta, kad draudimo tvarkyti specialiųjų kategorijų asmens duomenis duomenų subjektas negali panaikinti (BDAR 9 str. 2 d. a p.).
[18] Tvarkyti duomenis būtina dėl svarbaus viešojo intereso priežasčių, remiantis Sąjungos arba valstybės narės teise, kurie turi būti proporcingi tikslui, kurio siekiama, nepažeisti esminių teisės į duomenų apsaugą nuostatų ir kuriuose turi būti numatytos tinkamos ir konkrečios duomenų subjekto pagrindinių teisių ir interesų apsaugos priemonės (BDAR 9 str. 2 d. g p.).

3. BDAR 22 STRAIPSNIO PROBLEMATIKA DI NAUDOJIMO KONTEKSTE

Daugelis sprendimų, kuriuos šiandien priima DI sistemos, patenka į BDAR 22 straipsnio 1 dalies taikymo sritį, nes DI algoritmai vis dažniau taikomi įdarbinimo, skolinimo, draudimo, sveikatos paslaugų, socialinės apsaugos, švietimo ir kt. srityse. (Sartor, 2020, p. 60), todėl šiame skyriuje bus siekiame pateikti tam tikrus probleminius aspektus, kylančius iš šio straipsnio taikymo duomenų valdytojams, naudojantiems DI. Šiame skyriuje bus kalbama tik apie BDAR 22 straipsnio problematiką tų DI technologijų atžvilgiu, kurios išpildo BDAR 21 straipsnio 1 dalies taikymo sąlygas (šio darbo 2.2 skyrius).

3.1. Tinkamų duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonių užtikrinimo problematika DI kontekste

BDAR 22 straipsnio 3 dalyje įtvirtinta, kad tais atvejais, kai duomenų valdytojai priimdami BDAR 22 straipsnio 1 dalyje nurodytus sprendimus remiasi sutarties (BDAR 22 straipsnio 1 dalies a punktas) ar sutikimo (BDAR 22 straipsnio 2 dalies c punktas) išimtimis, duomenų valdytojai turi įgyvendinti tinkamas priemones, kad būtų apsaugotos duomenų subjekto teisės bei laisvės ir teisėti interesai, bent 1) teisė iš duomenų valdytojo reikalauti žmogaus įsikišimo, 2) teisė pareikšti savo požiūrį ir 3) teisė užginčyti sprendimą. Žodis „bent“ reiškia, kad straipsnyje minimos konkrečios duomenų subjektų apsaugos priemonės turi būti įgyvendintos visais atvejais, kai duomenų valdytojas priima BDAR 22 straipsnio 1 dalyje nurodytus sprendimus ir remiasi sutarties ar sutikimo išimtimis. DI naudojimo kontekste specifikos užtikrinant duomenų subjektų teisę pareikšti savo požiūrį nėra, todėl autoriaus pasirinkimu šiame skyriuje toliau bus analizuojamos šios dvi duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonės, kurias užtikrinant praktikoje naudojant DI gali kilti tam tikros problemos – 1) teisė pareikšti savo požiūrį ir 2) teisė užginčyti sprendimą.

3.1.1. Teisė reikalauti žmogaus įsikišimo

BDAR 22 straipsnio 1 dalis taikoma tik tais atvejais, kai sprendimas yra priimamas tvarkant duomenis tik automatizuotu būdu (be žmogaus įsikišimo). Tam, kad BDAR 22 straipsnio 1 dalis nebūtų taikoma, žmogaus dalyvavimas sprendimo priėmimo procese negali būti fiktyvus – jis iš tikrųjų turi turėti galimybę daryti įtaką priimam sprendimui. Iš to seka, kad teise reikalauti žmogaus įsikišimo duomenų subjektui suteikiama galimybė pasirinkti, kad

jo atžvilgiu priimamo sprendimo procese (reikšmingai) dalyvautų žmogus. Kaip teigia M. Brkan, BDAR 22 straipsnis atspindi ES skepticizmą dėl šališkumo ir galimai klaidingų sprendimų, kurie gali būti priimami automatizuotomis priemonėmis, jei jų nepatikrina žmonės (Brkan, 2018, p. 7). Kita vertus, šia nuostata, kuria duomenų subjektui suteikiamos tam tikros garantijos, visų pirma teisė į žmogaus įsikišimą, sprendžiami susirūpinimą keliantys klausimai, susiję su nepakankamomis duomenų subjektų galimybėmis daryti įtaką sprendimams, kurie vis dažniau priimami automatizuotomis priemonėmis (Mendoza, Bygrave, 2017, p. 8).

Kaip teigia M. Almada, tyliosios žmogaus žinios (angl. *tacit human knowledge*) ir intuicijos, kurias gali būti sudėtinga pateikti kompiuteriniu būdu, gali padėti nustatyti mašinų padarytas klaidas. Žvelgiant iš instrumentinės perspektyvos (angl. *instrumental perspective*), žmogaus dalyvavimas reikalingas kaip kokybės kontrolė, ypač dėl to, kad automatizuotų sistemų klaidos gali sukelti didelio masto žalą[19] (Almada, 2019, p. 3). Vis dėl to, galima užimti ir priešingą poziciją, kad žmogaus rėmimasis savo intuicija ir „tyliosiomis žiniomis“ gali sudaryti prielaidas, pavyzdžiui, diskriminacijos apraiškoms, dėl žmonėms būdingų kognityvinio šališkumo, kuris lemia sistemingas vertinimo ir sprendimų priėmimo klaidas (Trazzi ir Yampolskiy, 2018, p. 1).

Taigi, teise reikalauti žmogaus įsikišimo siekiama sumažinti rizikas, galinčias kilti duomenų subjektams iš jų atžvilgių priimamų sprendimų, grindžiamų tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, tačiau galima suabejoti, ar „žmogaus įsikišimas“ į sprendimo priėmimo procesą yra tinkama ir efektyvi priemonė mažinti iš BDAR 22 straipsnio 1 dalyje nurodyto asmens duomenų tvarkymo kylančias rizikas, kadangi tam tikrais atvejais žmogaus įsikišimas gali būti net ir žalingas.

Reikia pripažinti, kad „žmogus įsikišimo“ nauda (ar žala) priklausys nuo konkrečios situacijos aplinkybių, todėl vienareikšmių išvadų daryti negalima. Visgi, galima šį problemiškumą iliustruoti pavyzdžiais. 2021 m. birželį Italijos priežiūros institucija Garante per la protezione dei dati personali (toliau – Garante) priėmė sprendimą skirti 2,6 mln. eurų baudą maisto pristatymo į namus bendrovei (toliau – Bendrovė), *inter alia*, už BDAR 22 straipsnio 3 dalies pažeidimą. Bendrovė, organizuodama darbuotojų darbą, taikė

[19] K. Brennan–Marquez ir S. Henderson pateikia dramatišką, tačiau iliustratyvų tokios situacijos pavyzdį – 1983 m. rugsėjo 26 d. priimtą Stanislovo Petrovo sprendimą panaikinti sovietų sistemos, kuri klaidingai aptiko branduolinę ataką, veikimą. Gavęs pranešimą iš palydovinio ryšio kompiuterių apie artėjančią JAV raketą, Petrovas nujautė, kad kažkas negerai, todėl pranešė apie sistemos gedimą. Kai vis pasirodė panašūs pranešimai – apie antrą, trečią, ketvirtą ir penktą branduolinę raketą, kurios visos turėjo atskristi per dvylika minučių – Petrovo nuojauta jam sakė tą patį, todėl jis vėl pranešė apie gedimą. Petrovas buvo teisus: palydovus suklaidino saulės atspindžiai, nors tuo metu jis to visiškai nežinojo. Jis tiesiog jautė, kad kažkas „ne taip", ir ši nuojauta galėjo padėti išvengti pražūtingo branduolinio karo (Brennan–Marueqz, Henderson, 2019, p. 146).

diskriminacines DI technologijas – Bendrovės maisto pristatymo į namus platformoje darbuotojams būdavo priskiriami užsakymai pagal tai, kaip jų darbą įvertindavo algoritmas t. y. darbuotojai, kurie turėdavo aukštesnį įvertinimą, turėdavo pirmumą prieš darbuotojus, kurių įvertinimas buvo mažesnis. Algoritmo veikimas didžiąja dalimi buvo pagrįstas klientų ir restoranų atsiliepimais bei pristatymo laiku, tačiau neigiami atsiliepimai turėdavo didesnį svorį, nei teigiami ir sistema bausdavo vairuotojus, jeigu jie neišpildydavo maisto pristatymui keliamų kriterijų (pvz., jeigu užsakymas buvo pristatomas ne laiku). Garante nusprendė, kad Bendrovė pažeidė BDAR 22 straipsnio 3 dalies reikalavimus, kadangi neužtikrino darbuotojams teisės reikalauti žmogaus įsikišimo ar užginčyti tik automatizuotu būdu priimtą sprendimą ir dėl to tam tikrais atvejais klientams palikus nepagrįstus atsiliepimus, kai kurie darbuotojai prarasdavo galimybę dirbti. Tokioje situacijoje teisė reikalauti žmogaus įsikišimo gali atnešti akivaizdžią naudą duomenų subjektui – atsakingam asmeniui nebūtų sudėtinga peržiūrėti (išsiaiškinti) kodėl klientas paskyrė vairuotojui neigiamą įvertinimą ir, jei paaiškėtų, kad toks įvertinimas nėra pagrįstas, jo rezultatus anuliuoti, tuo pačiu anuliuojant ir iš tik automatizuotu būdu priimto sprendimo kylančias neigiamas pasekmes duomenų subjektui. Žmogaus įsikišimas į DI priimamą sprendimą gali sukelti ir neigiamas pasekmes duomenų subjektui, pavyzdžiui, DI diagnozuodamas ligas ar siūlantis individualų gydymą gali remtis dideliais informacijos kiekiais, pavyzdžiui, paciento šeimos narių ligų istorija, ankstesnių pacientų įrašais, susiejant jų charakteristikas ir medicininius tyrimus su vėlesnėmis sveikatos būklėmis ir gydymu (Sartor, 2020, p. 16). Abejotina, kad žmogus galėtų apdoroti tokius didelius informacijos kiekius, todėl gali susidaryti paradoksali situacija, kuomet duomenų subjektas, tikėdamasis, kad pasinaudojus teise reikalauti žmogaus įsikišimo, jo individuali situacija bus išnagrinėta detaliau ir, atitinkamai, bus priimtas „mažiau pavojų keliantis“ sprendimas, gali sulaukti priešingo rezultato, kad žmogus šią užduotį atliks ne taip tiksliai ir su didesne tikimybe kilti pavojams duomenų subjekto teisėms, laisvėms ir teisėtiems interesams.

3.1.2. Teisė užginčyti sprendimą

BDAR 22 straipsnio 3 dalyje įtvirtinta, kad duomenų subjektas turi teisę užginčyti jo atžvilgiu priimtą sprendimą. Terminas „ginčyti" reiškia daugiau nei „prieštarauti" ar „nesutikti" <...> ir yra artimas teisei į apeliaciją (angl. *akin to a right of appeal*) (Mendoza, Bygrave, 2017, p. 16). Duomenų valdytojas turi užtikrinti, kad duomenų subjektui pareikalavus sprendimas, nurodytas BDAR 22 straipsnio 1 dalyje, būtų peržiūrėtas. Anot

29 straipsnio darbo grupės, sprendimą peržiūrintis asmuo turėtų kruopščiai įvertinti visus susijusius duomenis, įskaitant visą papildomą informaciją, kurią pateikia duomenų subjektas (29 straipsnio darbo grupės gairės, 2018, p. 29).

Kaip teigia M. Brkan, praktiškai tai reiškia, kad procedūra tampa rungtyniška (angl. *adverserial*), ir, atsižvelgiant į tai, kyla klausimas, kas turėtų priimti sprendimą dėl tokio duomenų subjekto prieštaravimo. Jei, pavyzdžiui, duomenų subjektas davė aiškų sutikimą automatizuotai vertinti jo kredito reitingą, o vėliau prieštarauja tokiam sprendimui, ar šį prieštaravimą turėtų nagrinėti bylą tvarkantis banko darbuotojas, kitas šios organizacijos darbuotojas, ar nepriklausoma institucija? (Brkan, 2018, p. 13). Šiuo klausimu teismų ar priežiūros institucijų praktikos nėra, taip pat jis nėra nagrinėtas plačiau ir teisės doktrinos atstovų darbuose. Visgi, remiantis atskaitomybės principu (BDAR 5 str. 2 d.), duomenų valdytojas pats turėtų pasirinkti, kokiu būdu konkrečioje situacijoje yra tikslinga užtikrinti duomenų subjekto teisę užginčyti sprendimą, kadangi priežiūros institucijai ar teismui pareikalavus, duomenų valdytojas privalėtų sugebėti įrodyti, kad procedūra nebuvo fiktyvi.

Akivaizdu, kad teisės užginčyti sprendimą įgyvendinimas duomenų valdytojui naudojančiam DI pareikalautų žmogiškųjų (taigi, ir finansinių) išteklių, kurių dydis priklausytų tiek nuo duomenų subjektų, siekiančių įgyvendinti šią savo teisę, skaičiaus, tiek nuo pačio automatizuoto sprendimo sudėtingumo, o tiksliau, nuo laiko, kurį sprendimo peržiūrėjimui turi skirti sprendimą peržiūrintis subjektas. Atitinkamai, duomenų valdytojai, ypač mažos ir vidutinės įmonės, gali būti atgrasytos nuo DI sistemų naudojimo savo veikloje, kadangi tokių sistemų naudojimas BDAR prasme kelia papildomų kaštų rizikas.

Apibendrinant šio darbo 3.1 skyrių, darytina išvada, kad viena vertus, teisės reikalauti žmogaus įsikišimo užtikrinimu siekiama sumažinti rizikas, kylančias iš be žmogaus įsikišimo atliekamo sprendimų priėmimo, kita vertus, galima suabejoti, ar teisė reikalauti žmogaus įsikišimo DI naudojimo kontekste yra tinkama priemonė šioms rizikoms sumažinti, kadangi tam tikrais atvejais šios teisės įgyvendinimas gali duomenų subjektui sukelti neigiamas pasekmes. BDAR nėra įtvirtinta, kaip turėtų būti užtikrinimas teisės užginčyti sprendimą įgyvendinimas, todėl pareiga užtikrinti šios teisės įgyvendinimą ir įrodyti, kad ši teisė buvo užtikrinta, remiantis atskaitomybės principu, tenka duomenų valdytojams, naudojantiems DI. Tiek teisės reikalauti žmogaus įsikišimo, tiek teisės užginčyti sprendimą įgyvendinimas reikalauja papildomų kaštų iš duomenų valdytojų, kurie privalo šias duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemones užtikrinti, todėl duomenų valdytojai gali būti atgrasyti nuo DI naudojimo savo veikloje.

3.2. Ar egzistuoja teisė gauti paaiškinimą?

BDAR preambulės 71 punkte įtvirtinta, kad atliekant duomenų tvarkymą, kaip nurodyta BDAR 22 straipsnio 1 dalyje, turėtų būti taikomos tinkamos apsaugos priemonės, įskaitant 1) konkrečios informacijos duomenų subjektui suteikimą ir 2) teisę reikalauti žmogaus įsikišimo, 3) pareikšti savo požiūrį, 4) gauti sprendimo, priimto atlikus šį vertinimą, paaiškinimą ir 5) teisę ginčyti tą sprendimą. Taigi, BDAR konstatuojamojoje dalyje yra įtvirtintos dvi papildomos (lyginant su BDAR 22 straipsnio 3 dalimi) duomenų subjektų apsaugos priemonės: 1) konkrečios informacijos duomenų subjektui suteikimas ir 2) teisė gauti sprendimo, atlikus šį vertinimą, paaiškinimą (toliau – teisė gauti paaiškinimą). BDAR preambulės 71 punkte įtvirtintas reikalavimas pateikti duomenų subjektui konkrečią informaciją persidengia su BDAR 13–15 straipsniais t. y. šiuose straipsniuose eksplicitiškai įtvirtinta, kokia informaciją turi būti pateikta duomenų subjektui[20], tačiau teisė gauti paaiškinimą BDAR nėra įtvirtinta. Kyla klausimas, ar BDAR preambulėje įtvirtinta teisė gauti paaiškinimą sukelia pareigą duomenų valdytojams kiekvienu atveju, kai duomenų subjektas pareikalauja žmogaus įsikišimo, pateikti duomenų subjektams paaiškinimą dėl sprendimo, kuris buvo priimtas BDAR 22 straipsnio 1 dalyje nurodytu būdu?

2016 m. priėmus BDAR, klausimas dėl teisės gauti paaiškinimą (ne)egzistavimo sulaukė (ir šiuo metu sulaukia) itin daug dėmesio iš teisės mokslo doktrinos atstovų[21]. Visgi, mokslininkai prieina skirtingų išvadų. Vieni teigia, kad teisė gauti paaiškinimą yra privaloma, nors ir nėra eksplicitiškai įtvirtinta pačiame BDAR, kiti teigia, kad tokios teisės BDAR duomenų subjektams nesuteikia. Prieš pradedant analizuoti teisės gauti paaiškinimą ne(egzistavimo) klausimą visų pirma tikslinga apsibrėžti teisės gauti paaiškinimą turinį. Kaip teigia S. Wachter et. al., gali būti svarstomi dviejų rūšių paaiškinimai, priklausomai nuo to, ar kalbama apie:

- sistemos funkcionalumą, t. y. logiką, reikšmę, numatomus padarinius ir bendrą automatinio sprendimų priėmimo sistemos funkcionalumą, pvz., sistemos reikalavimų

[20] Duomenų valdytojai turi pateikti informaciją dėl to, kad esama 22 straipsnio 1 ir 4 dalyse nurodyto automatizuoto sprendimų priėmimo, įskaitant profiliavimą, ir, bent tais atvejais, prasmingą informaciją apie loginį jo pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui (BDAR 13 str. 2 d. f p., 14 str. 2 d. g p. ir 15 str. 1 d. h p.).

[21] Šį klausimą nagrinėjo tokie autoriai kaip B. Casey et. Al. (Casey et. al. 2018), R. Hamon et. al. (Hamon et al., 2021), D. Sancho (Sancho, 2020), L. Edwards ir M. Veale (Edwards and Veale, 2017), S. Wachter et. al. (Wachter et. al. 2016), B. Goodman ir S. Flaxman (Goodman ir Flaxman, 2017), M. Brkan (Brkan, 2017), G. Sartor (Sartor, 2020)ir kt.

specifikaciją, sprendimų medžius (angl. *decision trees*), iš anksto nustatytus modelius, kriterijus ir klasifikavimo struktūras, arba

- konkrečius sprendimus, t. y. konkretaus automatizuoto sprendimo pagrindimą, priežastis ir individualias aplinkybes, pvz., požymių svorį sprendimo priėmimo procese, mašinos nustatytas konkretaus atvejo (angl. *machine–defined case–specific*) sprendimo taisykles, informaciją apie profilių, kuriems gali būti priskiriami duomenų subjektai, grupes (Wachter et. al. 2016, p. 78).

Autoriaus nuomone, kai kalbame apie teise gauti paaiškinimą, turėtume ją suprasti kaip konkretaus BDAR 22 straipsnio 1 dalyje nurodytu būdu priimto sprendimo paaiškinimą, kadangi sistemos funkcionalumo paaiškinimas jau yra padengtas BDAR 13–15 straipsniuose įtvirtintomis pareigomis t. y. reikalavimu nurodyti prasmingą informaciją apie sprendimo loginį pagrindimą ir numatomas pasekmes duomenų subjektui. Remiantis tokiu aiškinimu, jeigu priežiūros institucijos ar teismai nuspręstu, kad BDAR suteikia duomenų subjektams teisę gauti paaiškinimą, tuomet ši teisė turėtų būti suprantama kaip *ex post* teisė į paaiškinimą t. y. kaip teisė gauti paaiškinimą dėl individualaus, jau priimto tik automatizuotu duomenų tvarkymu grindžiamo sprendimo. Identifikavus teisės į paaiškinimą turinį, tikslinga pateikti argumentus dėl šios teisės (ne)egzistavimo.

I. Mendoza ir L. A. Bygrave teigia, kad teisė gauti paaiškinimą yra numanoma teisėje „užginčyti" sprendimą pagal BDAR 22 straipsnio 3 dalį: kad apeliacinis procesas duomenų subjektui pasinaudojus teise užginčyti sprendimą būtų iš tiesų teisingas, jame papildomai turi būti numatyta duomenų valdytojo pareiga pateikti apeliantui sprendimo motyvus (Mendoza, Bygrave, 2017, p. 17). M. Brkan teigimu, atsižvelgiant į tai, kad pagal BDAR skaidrumas yra susijęs su konkrečiu asmeniu <...> jis gali būti suprantamas kaip „individualus skaidrumas", nes pagal jį duomenų subjektui iš esmės suteikiama teisė gauti paaiškinimą ir suprasti sprendimo priėmimo priežastis automatizuoto duomenų tvarkymo atveju (Brkan, 2018, p. 14).

Tuo tarpu S. Wachter teigimu, teisė gauti paaiškinimą nėra paminėta tarp teisių, kurias duomenų valdytojas turi minimaliai užtikrinti, kad nepažeistų BDAR 22 straipsnio 3 dalies, iš to seka, kad negalima laikyti, kad teisė gauti paaiškinimą yra privaloma. Būtų labai prieštaringa skirti baudas duomenų valdytojams iš anksto aiškiai ir neabejotinai nepaaiškinus, kokių pareigų turi būti laikomasi ir atrodo, kad teisė į paaiškinimą BDAR 22 straipsnyje praleista sąmoningai. BDAR preambulės 71 punkte nurodytos apsaugos priemonės yra beveik identiškos BDAR 22 straipsnio 3 dalyje nurodytoms apsaugos priemonėms, tik su tuo esminiu skirtumu, kad į BDAR preambulės 71 punktą papildomai įtraukta teisė „gauti sprendimo, priimto atlikus šį vertinimą, paaiškinimą". Tikslingas šio

teksto neįtraukimas į BDAR 22 straipsnį gali būti ne neapsižiūrėjimas, bet rodo, kad teisės aktų leidėjai neketino BDAR įtvirtinti teisės į konkrečių sprendimų paaiškinimą (Wachter et. al. 2016, p. 80). L. Edwards ir M. Veale požiūriu, teisė gauti sprendimo paaiškinimą yra įtvirtinta tik BDAR preambulės 71 punkte ir <...> nors konstatuojamosios dalys yra teisės akto teksto dalis, manoma, kad jos aiškina pagrindinį tekstą, o ne sukuria savarankiškus papildomus įsipareigojimus[22] (Edwards ir Veale, 2018, p. 49–50).

Anot G. Sartor, galimi du aiškinimai: remiantis pirmuoju aiškinimu, ES teisės aktų leidėjas, įtraukdamas reikalavimą pateikti konkretų paaiškinimą tik į BDAR preambulę ir neįtraukdamas jo į BDAR straipsnius, siekė perduoti dvigubą žinią: netaikyti vykdytinos teisinės prievolės teikti konkrečius paaiškinimus ir kartu rekomenduoti, kad duomenų valdytojai tokius paaiškinimus teiktų, kai jiems tai patogu, vadovaudamiesi savo nuožiūra. Pagal šį aiškinimą individualių paaiškinimų teikimas būtų tik geroji praktika, o ne teisiškai vykdytinas reikalavimas. Remiantis antruoju aiškinimu, ES teisės aktų leidėjas, priešingai, siekė nustatyti vykdytiną teisinę prievolę pateikti individualų paaiškinimą, nors ir pernelyg neapsunkindamas duomenų valdytojų. Šį aiškinimą nurodo sąlyginis žodis „bent jau", esantis prieš nuorodą į „teisę į žmogaus įsikišimą iš duomenų valdytojo pusės, teisę išreikšti savo požiūrį ir užginčyti sprendimą". Atrodo, kad šis patikslinimas leidžia manyti, jog kai kurie paslaugų teikėjai teisiškai privalo taikyti papildomas apsaugos priemones, galbūt įskaitant individualizuotus paaiškinimus, kaip nurodyta BDAR preambulės 71 punkte. Laikantis šio antrojo požiūrio, paaiškinimas būtų teisiškai būtinas, kai tai praktiškai įmanoma, t. y. kai tai suderinama su technologijomis, sąnaudomis ir verslo praktika (Sartor, 2020, p. 63).

Autoriaus požiūriu, papildomai verta atkreipti dėmesį į teisėtumo, sąžiningumo ir skaidrumo principą (BDAR 5 str. 1 d. a p.) – tai pamatinis, plačiausias ir abstrakčiausias duomenų apsaugos teises principas. Šio principo dėmenis – teisėtumą, sąžiningumą ir skaidrumą – galima laikyti atskirais duomenų apsaugos teises principais (Zaleskis, 2018, p. 79). Kalbant apie duomenų valdytojų pareigą pateikti individualų priimto sprendimo paaiškinimą, ypač svarbus skaidrumo principas. Anot 29 straipsnio darbo grupės skaidrumas <...> suteikia duomenų subjektams galimybę <...> kontroliuoti savo asmens duomenis, pavyzdžiui, <...> naudojantis savo duomenų subjekto teisėmis (Article 29 Working Party Guidelines On Transparency, 2018, p. 6). Vaduojantis šia logika, duomenų subjekto teisė gauti individualų paaiškinimą suteiktų jam galimybę pasinaudoti, pavyzdžiui, teise užginčyti sprendimą (BDAR 22 straipsnio 3 dalis), kadangi nežinodamas

[22] Prie šio argumento dar galima pridėti ir T. Klimo bei J. Vaičiukaitės išsakytą mintį, kad ES teisės akto preambulė neturi privalomos teisinės galios (Klimas, Vaičiukaitė, 2008, p. 25).

jo atžvilgiu priimto sprendimo motyvų, duomenų subjektas prarastų galimybę duomenų valdytojui pateikti konkrečius argumentus, kodėl duomenų subjekto manymu, jo atžvilgiu yra priimtas netinkamas sprendimas. Todėl, nors teisė gauti individualų paaiškinimą yra įtvirtinta tik BDAR preambulėje (formaliuoju požiūriu nėra privaloma), visgi, remiantis teisėtumo, sąžiningumo ir skaidrumo principu (BDAR 5 str. 1 d. a p.) bei atskaitomybės principu (BDAR 5 str. 2 d.), duomenų valdytojai praktikoje šią teisę veikiausiai turėtų užtikrinti bent tais atvejais, kai duomenų subjektams sprendimo paaiškinimas būtų reikalingas siekiant pasinaudoti kitomis BDAR įtvirtintomis teisėmis, pavyzdžiui, teise užginčyti sprendimą.

Kokią praktinę įtaką DI savo veikloje naudojantiems duomenų valdytojams turėtų teisės gauti paaiškinimą privalomas pobūdis? Sudėtingų DI technologijų, pavyzdžiui, mašininiu mokymusi (angl. *machine learning*) ar giliuoju mokymusi (angl. *deep learning)* paremtų DI technologijų veikimas yra toks sudėtingas, kad net patys duomenų valdytojai ne visais atvejais gali tiksliai pasakyti, kokiu būdu DI priėmė vienokį ar kitokį sprendimą. Techninių kliūčių, trukdančių paaiškinti algoritmais pagrįstus sprendimus, skaičius priklauso nuo algoritmo sudėtingumo (Brkan, 2017, p. 21). Kaip teigia R. Hamon et. al., galimybė pateikti pakankamai informatyvų ir skaidrų paaiškinimą priklauso ir nuo galimybės įrodyti priežastinį ryšį tarp įvesties duomenų (angl. *input data*) ir galutinio sprendimo. Tačiau tai ne visada įmanoma <...> priimant sudėtingesnius dirbtiniu intelektu grindžiamus sprendimus gali būti sunku pasiekti pakankamą algoritmų skaidrumą. Visų pirma, vis dažniau taikant gilųjį mokymąsi vis daugiau automatizuotų sprendimų formų, sunku tiksliai paaiškinti konkrečių priimtų sprendimų priežastis <...> pastaraisiais atvejais galimų paaiškinimų kokybė gali būti laikoma nepakankama pagal BDAR 22 straipsnio 3 dalį. Jei laikytumėmės griežto požiūrio, tai reikštų, kad arba technologiškai pažangesnės (ir neaiškios) sprendimų priėmimo formos turėtų būti uždraustos, nes jų neįmanoma paaiškinti, arba, kad turėtume toleruoti DI grindžiamas sprendimų priėmimo sistemas, kuriose formaliai nesilaikoma BDAR nustatytų skaidrumo pareigų (Hamon et al., 2021, p. 558).

Apibendrinant, darytina išvada, kad reikalauti iš duomenų valdytojo paaiškinimo, kodėl jo naudojamas DI priėmė tam tikrą sprendimą, būtų beveik neįmanoma užduotis, ypač individualiu lygmeniu, kadangi DI priimą neišmatuojamą skaičių mikrosprendimų, pagrįstų dideliais duomenų rinkiniais ir nuolat besimokančiu algoritmu. Sutiktina su R. Hamon et. al. pozicija, kad jeigu būtų pripažintas teisės gauti paaiškinimą privalomas pobūdis, duomenų valdytojai turėtų rinktis arba nenaudoti pažangių ir sudėtingų DI technologijų, kurių priimamus sprendimus ne visais atvejais galima paaiškinti, arba

prisiimti iš BDAR kylančias baudų rizikas. Tokia situacija gali atgrasyti duomenų valdytojus nuo DI naudojimo savo veikloje, todėl sprendžiant teisės gauti paaiškinimą (ne)egzistavimo klausimą ypatingas dėmesys turėtų būti skiriamas BDAR preambulės 4 punktui – asmens duomenys turėtų būti tvarkomi taip, kad tai pasitarnautų žmonijai. Teisė į asmens duomenų apsaugą nėra absoliuti; ji turi būti vertinama atsižvelgiant į jos visuomeninę paskirtį ir derėti su kitomis pagrindinėmis teisėmis, remiantis proporcingumo principu. Šiuo reglamentu paisoma visų Chartijoje pripažintų ir Sutartyse įtvirtintų pagrindinių teisių ir laisvių bei principų, visų pirma teisės į <...> saviraiškos ir informacijos laisvės, laisvės užsiimti verslu. Taigi, teisės gauti paaiškinimą klausimas ir kiti klausimai turi būti sprendžiamas platesniame nei tik duomenų apsaugos teisė, kontekste, kadangi besąlygiškai pripažinus duomenų subjektų teisę gauti paaiškinimą būtų apsunkinta duomenų valdytojų, savo veikloje naudojančių sudėtingas DI technologijas, padėtis. Pripažinus teisę gauti paaiškinimą, be abejo, būtų sustiprintas duomenų apsaugos lygis ES, tačiau reikia nepamiršti, kad duomenų apsaugos teisė turi būti derinama su kitomis ES pripažįstamomis vertybėmis, *inter alia,* socialine bei ekonomine pažanga, prie kurios stiprinimo DI neabejotinai prisideda.

IŠVADOS

1. Automatizuotų sprendimų sąvoka yra susijusi su sprendimo dėl duomenų subjekto priėmimo būdu. Tuo tarpu profiliavimo sąvoka yra susijusi su asmens elgesio prognozavimu pagal tam tikras koreliacijas tarp duomenų, surinktų apie šį asmenį ir duomenų, turimų apie kitus asmenis. Nors automatizuotų sprendimo priėmimo ir profiliavimo sąvokos yra skirtingos, tačiau dažnu atveju šios sąvokos papildo viena kitą t. y. automatizuoti sprendimai gali būti grindžiami profiliavimu ar iš dalies sutapti su profiliavimu.
2. Egzistuoja dviprasmiškumo problema BDAR 22 straipsnio 1 dalies interpretavimo atžvilgiu. Nėra teisinio aiškumo dėl to, ar BDAR 22 straipsnio 1 dalyje įtvirtinta teisė turėtų būti interpretuojama kaip teisė, kuria duomenų subjektai turi aktyviai pasinaudoti, ar kaip bendras draudimas tvarkyti duomenis.
3. Įvairios sąlygos, kurias duomenų valdytojai turi išpildyti, norėdami pasinaudoti BDAR 22 straipsnio 2 dalyje įtvirtintomis išimtimis, ypač DI naudojimo kontekste, apsunkina duomenų valdytojams galimybę remtis šiomis išimtimis priimant tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamus sprendimus. Visgi, BDAR 22 straipsnio 2 dalies b punktas įtvirtina plačią diskreciją ES valstybių narių įstatymų leidėjams reguliuoti BDAR 22 straipsnio 1 dalyje aprašytus automatizuotus sprendimus nacionaliniu lygmeniu.
4. Situacijose, kai naudojamas DI, dėl žmogui būdingo kognityvinio šališkumo ir didelio DI apdorojamo duomenų kiekio galima suabejoti žmogaus įsikišimo, kaip duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonės, nauda.
5. Teisė gauti paaiškinimą formaliuoju požiūriu nėra privaloma, tačiau remiantis BDAR įtvirtintais principais, duomenų valdytojai praktikoje šią teisę turėtų užtikrinti bent tais atvejais, kai duomenų subjektams sprendimo paaiškinimas būtų reikalingas siekiant pasinaudoti kitomis BDAR įtvirtintomis teisėmis, pavyzdžiui, teise užginčyti sprendimą.
6. Duomenų valdytojams, ypač tais atvejais, kai yra naudojamos sudėtingos DI technologijas, praktiškai gali būti neįmanoma įgyvendinti teisės gauti paaiškinimą (jei tokia teisė būtų pripažinta). Jeigu būtų pripažintas teisės gauti paaiškinimą privalomas pobūdis, duomenų valdytojai turėtų rinktis arba nenaudoti pažangių ir sudėtingų DI technologijų, kurių priimamus sprendimus ne visais atvejais galima paaiškinti, arba prisiimti iš BDAR kylančias baudų rizikas.

ŠALTINIŲ SĄRAŠAS

TEISĖS NORMINIAI AKTAI

1. 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).
2. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR, OL L 119, 2016 5 4.
3. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL 2004 m. specialusis leidimas*, 13 skyrius, 15 tomas, p. 355–374.

SPECIALIOJI LITERATŪRA

4. Almada, M. (2019). *Human intervention in automated decision–making: Toward the construction of contestable systems.* In Proceedings of the Seventeenth International Conference on Artificial Intelligence and Law.
5. Brkan, M. (2017). *Do Algorithms Rule the World? Algorithmic Decision–Making in the Framework of the GDPR and Beyond* [interaktyvus]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901> [žiūrėta 2022 m. vasario 23 d.].
6. Casey, B., Farhangi, A. and Vogl, R. (2018). *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise* [interaktyvus]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3143325> [žiūrėta 2022 m. balandžio 2 d.].
7. Edwards, L. and Veale, M. (2017). *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For* [interaktyvus]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2972855> [žiūrėta 2022 m. balandžio 11 d.].
8. Ehteshami Bejnordi, B., Veta, M., Johannes van Diest, P., van Ginneken, B., Karssemeijer, N., Litjens, G., van der Laak, J.A.W.M., Hermsen, M., Manson, Q.F., Balkenhol, M., Geessink, O., Stathonikos, N., van Dijk, M.C., Bult, P., Beca, F., Beck,

A.H., Wang, D., Khosla, A., Gargeya, R. and Irshad, H. (2017). *Diagnostic Assessment of Deep Learning Algorithms for Detection of Lymph Node Metastases in Women With Breast Cancer. JAMA*, 318(22), p. 2199.

9. Falletti, E. (2019). *Automated Decisions and Article No. 22 GDPR of the European Union: An Analysis of the Right to an 'Explanation'*. Available at SSRN 3510084.
10. Gillham, J., Rimmington, L., Dance, H., Verweij, G., Rao, A., Roberts, K.B. and Paich, M. (2018). *The macroeconomic impact of artificial intelligence.* PwC Report–PricewaterhouseCoopers.–2018.
11. Goodman, B. and Flaxman, S. (2017). *European Union Regulations on Algorithmic Decision–Making and a "Right to Explanation."*. AI Magazine, 38(3), p. 50–57.
12. Hamon, R., Junklewitz, H., Malgieri, G., De Hert, P., Beslay, L. and Sanchez, I. (2021). *Impossible Explanations? Beyond explainable AI in the GDPR from a COVID–19 Use Case Scenario* [interaktyvus]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3774114> [žiūrėta 2022 m. kovo 31 d.].
13. Humerick, M. (2018). *Taking AI Personally: How the EU Must Learn to Balance the Interests of Personal Data Privacy & Artificial Intelligence*. 34 Santa Clara High Tech. L.J. 393, 2018 [interaktyvus]. Prieiga per internetą: <https://digitalcommons.law.scu.edu/chtlj/vol34/iss4/3/> [žiūrėta 2020–03–17].
14. Brennan–Marquez, K. and Henderson, S.E. (2018). *Artificial Intelligence and Role–Reversible Judgment* [interaktyvus]. Prieiga per internetą: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3224549> [žiūrėta 2022 m. balandžio 5 d.].
15. Klimas, T. and Vaiciukaite, J. (2008). *The law of recitals in European Community legislation*. ILSA J. Int'l & Comp. L., 15.
16. Koerner, K. (2018). *GDPR – boosting or choking Europe's data economy?* Deutsche Bank Research [interaktyvus]. Prieiga per internetą: <https://www.dbresearch.com/servlet/reweb2.ReWEB?rwsite=RPS_EN–PROD&rwobj=ReDisplay.Start.class&document=PROD0000000000470381#> [žiūrėta 2022 m. kovo 3 d.].
17. Kosinski, M., Stillwell, D. and Graepel, T. (2013). *Private traits and attributes are predictable from digital records of human behavior.* Proceedings of the National Academy of Sciences, 110(15), pp.5802–5805.

18. Kuner, C., Bygrave, L.A. and Docksey, C. (2019). *Commentary on the EU general data protection regulation (GDPR). A commentary*. Kettering: Oxford University Press.
19. McCarthy, J., Minsky, M.L., Rochester, N. and Shannon, C.E. (2006). *A proposal for the dartmouth summer research project on artificial intelligence*. AI magazine, 27(4), p.12–12.
20. Mendoza, I. and Bygrave, L.A. (2017). *The right not to be subject to automated decisions based on profiling.* In EU Internet Law (pp. 77–98). Springer, Cham.
21. MITROU, L. (2018). *Data Protection, Artificial Intelligence and Cognitive Services: Is the General Data Protection Regulation (GDPR) 'Artificial Intelligence–Proof'?* [interaktyvus]. Prieiga per internetą: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3386914 [žiūrėta 2022 balandžio 13].
22. Sancho, D. (2020). *Automated Decision–Making under Article 22 GDPR: Towards a More Substantial Regime for Solely Automated Decision–Making*. in Ebers, M. and Navas, S. (eds) Algorithms and Law. Cambridge: Cambridge University Press, pp. 136–156. doi: 10.1017/9781108347846.005.
23. Sarra, C. (2020). Defenceless? An Analytical Inquiry into The Right to Contest Fully Automated Decisions In the GDPR. An Anthology of Law, pp.235–252.
24. Sartor, G. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence: Study*. European Parliament.
25. Tosoni, L. (2021). *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation.* International data privacy law, 11(2), pp. 145–162. doi: 10.1093/idpl/ipaa024.
26. Trazzi, M. and Yampolskiy, R.V. (2018). *Building safer AGI by introducing artificial stupidity.* arXiv preprint arXiv:1808.03644.
27. Wachter, S., Mittelstadt, B. and Floridi, L. (2017). *Why a right to explanation of automated decision–making does not exist in the general data protection regulation*. International Data Privacy Law, 7(2), p. 76–99.
28. ZALESKIS, J. (2018). *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ Registrų centras, 2019.

TEISMŲ PRAKTIKA

Europos Sąjungos Teisingumo Teismo sprendimai

29. Breyer *prieš Vokietijos Federacinę Respubliką* [ESTT], Nr. C–582/14. [2016 m. spalio 16 d.]. ECLI:EU:C:2016:779.
30. *Heinz Huber prieš Vokietijos Federacinę Respubliką* [ESTT], Nr. C–524/06. [2008 m. gruodžio 16 d.]. ECLI:EU:C:2008:724.
31. *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde prieš Rīgas pašvaldības SIA „Rīgas satiksme“* [ESTT], Nr. C–13/16, [2017 m. sausio 26 d.]. ECLI:EU:C:2017:43.

Užsienio valstybių teismų praktika

32. Austrijos federalinio administracinio teismo (Bundesverwaltungsgericht) 2020 m. gruodžio 18 d. sprendimas. ECLI:AT:BVWG:2020:W256.2235360.1.00).
33. Hagos apygardos teismo (Rechtbank Den Haag) 2020 m. vasario 5 d. sprendimas nr. *DS89 – K477*. ECLI:NL:RBDHA:2020:865.

SOFT LAW

34. European Data Protection Board (2019). *Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects* [interaktyvus]. Prieiga per internetą: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines–art_6–1–b–adopted_after_public_consultation_en.pdf > [žiūrėta 2022 m. balandžio 5 d.].
35. European Data Protection Board (2020). *Guidelines 05/2020 on consent under Regulation 2016/679* [interaktyvus]. Prieiga per internetą: <https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf > [žiūrėta 2022 m. balandžio 7 d.].
36. Article 29 Data Protection Working Party (2017). *Guidelines on consent under Regulation 2016/679* [interaktyvus]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/items/623051/en> [žiūrėta 2022 m. balandžio 5 d.].
37. Article 29 Data Protection Working Party (2013). *Opinion 03/2013 on purpose limitation, 00569/13/EN WP 203* [interaktyvus]. Prieiga per internetą: <https://ec.europa.eu/justice/article–29/documentation/opinion–recommendation/files/2013/wp203_en.pdf> [žiūrėta 2022 m. balandžio 7 d.].
38. Article 29 Data Protection Working Party (2018). *Transparency Guidelines, wp260rev.01* [interaktyvus]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=51025> [žiūrėta 2022 m. kovo 17 d.].

39. Europos Komisija (2018). *Europos Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir regionų komitetui Dirbtinis intelektas Europai, COM/2018/237 final* [interaktyvus] Prieiga per internetą: <https://ec.europa.eu/transparency/regdoc/rep/1/2018/LT/COM–2018–237–F1–LT–MAIN–PART–1.PDF> [žiūrėta 2022 m. kovo 12 d.].
40. Article 29 Data Protection Working Party (2018). *Guidelines on Automated individual decision–making and Profiling for the purposes of Regulation 2016/679, WP251rev.01* [interaktyvus]. Prieiga per internetą: <https://ec.europa.eu/newsroom/article29/item–detail.cfm?item_id=612053> [žiūrėta 2022 kovo 16 d.].

KITI ŠALTINIAI

41. www.enforcementtracker.com. (n.d.). *GDPR Enforcement Tracker – list of GDPR fines*. [interaktyvus]. Prieiga per internetą: <https://www.enforcementtracker.com/?insights> [žiūrėta 2022 m. kovo 2 d.].
42. www.forbes.com. (n.d.). *54 Predictions About The State Of Data In 2021*. [interaktyvus] Forbes. Prieiga per internetą: https://www.forbes.com/sites/gilpress/2021/12/30/54–predictions–about–the–state–of–data–in–2021/?sh=2b3481e3397d [žiūrėta 2022 m. kovo 22 d.].
43. the Guardian. (2018). *The Cambridge Analytica Files | The Guardian* [interaktyvus]. Prieiga per internetą: <https://www.theguardian.com/news/series/cambridge–analytica–files> [žiūrėta 2022 m. kovo 3 d.].

SANTRAUKA

Automatizuotas sprendimų priėmimas pagal BDAR 22 straipsnį ir dirbtinis intelektas: taikymo prielaidos ir problematika

Arnas Malakauskas

Magistro darbe analizuojamas automatizuotas atskirų sprendimų priėmimas, įskaitant profiliavimą (BDAR 22 straipsnis) ir problematika, susijusi su šio straipsnio taikymu duomenų valdytojams, savo veikloje naudojantiems DI. Šie klausimai analizuojami nagrinėjant *soft law* šaltinius, skirtingas teisės doktrinos atstovų pozicijas ir teismų praktikoje pateiktus išaiškinimus. Darbe aptariamos profiliavimo ir automatizuotų sprendimų priėmimo sąvokos. Duomenų subjekto teisė nebūti automatizuotų sprendimų priėmimo subjektu (BDAR 22 straipsnio 1 dalis) analizuojama pateikiant šios teisės dviprasmiškumo problemą, taikymo sąlygas bei ribas. Darbe taip pat analizuojama problematika, susijusi su tinkamų duomenų subjektų teisių, laisvių ir teisėtų interesų apsaugos priemonių užtikrinimu, kai BDAR 22 straipsnio 1 dalyje nurodyti sprendimai priimami naudojant DI. Ši problematika labiausiai pastebima tuomet, kai yra naudojamos sudėtingos DI technologijos, kuomet žmogui dėl ribotų galimybių apdoroti didelius duomenų kiekius gali būti sudėtinga užtikrinti duomenų subjektų teisę reikalauti žmogaus įsikišimo ar užginčyti sprendimą. Darbe nagrinėjamas ir teisės gauti paaiškinimą klausimas, daroma išvada, kad jeigu būtų pripažintas tokios teisės privalomas pobūdis, duomenų valdytojai turėtų rinktis arba nenaudoti sudėtingų DI technologijų (kurių negalima paaiškinti), arba prisiimti iš BDAR kylančių baudų rizikas. Nagrinėjamos problematikos kontekste daroma išvada, kad teisė gauti paaiškinimą formaliuoju požiūriu nėra privaloma, tačiau remiantis BDAR įtvirtintais principais, duomenų valdytojai praktikoje šią teisę tam tikrais atvejais turėtų įgyvendinti.

SUMMARY

Automated Decision Making under Article 22 of the GDPR and Artificial Intelligence: Application Prerequisites and Issues

Arnas Malakauskas

The Master's thesis analyses automated individual decision–making, including profiling (Article 22 GDPR), and the issues related to the application of this Article to data controllers using AI in their activities. These issues are analysed by examining *soft–law* sources, different positions of authors in the legal field and interpretations in case law. The work clarifies the concepts of profiling and automated decision–making. The data subject's right not to be the subject to automated decision–making (Article 22(1) of the GDPR) is analysed by presenting the problem of the ambiguity of this right and the conditions and limits of its application. The work also analyses the issues related to ensuring adequate safeguards for the protection of the rights, freedoms and legitimate interests of data subjects when decisions referred to in Article 22(1) of the GDPR are taken by using AI. This issue is most pronounced when sophisticated AI technologies are used, where the limited ability of a human being to process large amounts of data may make it difficult to ensure the right to request human intervention or to challenge the decision. The paper also examines the issue of the right to obtain an explanation, concluding that, if such a right were to be recognised as mandatory, data controllers would have to choose between not using sophisticated AI systems (which cannot be explained) or bearing the risks of fines arising from the GDPR. In the context of the issues under examination, it is concluded that the right to obtain an explanation is not formally mandatory, but based on the principles enshrined in the GDPR, data controllers should, in practice, give effect to this right in certain cases.