Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Domantės Mozerytės,
V kurso, tarptautinės ir Europos Sąjungos
teisės šakos studentės

Magistro darbas

ES Bendrojo duomenų apsaugos reglamento principų problematika dirbtinio intelekto kontekste

Issue of the Principles of the EU General Data Protection Regulation in the Context of Artificial Intelligence

Vadovas: asist. dr. Julius Zaleskis
Recenzentė: asist. dr. Deimilė Prapiestytė

Vilnius
2023

ANOTACIJA IR PAGRINDINIAI ŽODŽIAI

Šiame darbe analizuojama Bendrojo duomenų apsaugos reglamento principų problematika dirbtinio intelekto kontekste. Pateikiamas dirbtinio intelekto apibrėžimas, atsižvelgiant į naujausią dirbtinio intelekto padėtį technologijų srityje. Nagrinėjamos aktualios Bendrojo duomenų apsaugos reglamento nuostatos dirbtiniam intelektui, kurios nulemia Bendrojo duomenų apsaugos reglamento principų taikymo sritį.

Pagrindiniai žodžiai: duomenų apsaugos teisė, Bendrasis duomenų apsaugos reglamentas, Bendrojo duomenų apsaugos reglamento principai, dirbtinis intelektas.

This thesis analyses the principles of the General Data Protection Regulation in the context of artificial intelligence. It provides a definition of artificial intelligence in the context of the latest state of the technology. It examines the relevant provisions of the General Data Protection Regulation for artificial intelligence, which determine the scope of the principles of the General Data Protection Regulation.

Keywords: data protection law, General Data Protection Regulation, principles of the General Data Protection Regulation, artificial intelligence.

TURINYS

ĮŽANGA

Temos aktualumas. Stebint naujausių skaitmeninių technologijų raidą, išryškėja tendencija, kad pasaulis stovi ant ketvirtosios pramonės revoliucijos slenksčio (Dogarua, 2020, p. 398). Palyginti su trimis ankstesnėmis revoliucijomis, ketvirtosios revoliucijos proveržį lemia asmens duomenys. Šią skaitmeninę transformaciją lemia pasaulinis mastas ir technologijų poveikis valstybėms, visuomenei, tarptautiniams santykiams ir aplinkai (Specialusis komitetas dirbtinio intelekto skaitmeniniame..., 2022, p. 10).

Dirbtinis intelektas – vienas iš pagrindinių polių, ant kurių stovi šiuolaikinis išmanusis technologijų pasaulis. Dirbtinis intelektas nėra naujiena daugelyje sričių. Dirbtinio intelekto taikymas apima įvairias sritis: mediciną, rinkodarą, finansus, aplinkosaugą, žemės ūkį. Kasdieniame gyvenime dirbtinį intelektą naudojame pasitelkdami integruotus išmaniuosius asistentus (pvz., „Google Assistant“ ar „Siri“), rašydami tekstus (pvz., naudodami programą „Grammarly“ siekdami patikrinti, ar tekste nėra gramatinių ir stiliaus klaidų) ar pasinaudodami internete rekomenduojamu turiniu (pvz., naudojantis „Spotify“ asmeniškai rekomenduojama muzika). Be to, kad dirbtinis intelektas palengvina kiekvieno asmens kasdienį gyvenimą, jis taip pat padeda spręsti įvairias visuomenės problemas: sparčiai diagnozuoja ligas, nuspėja kibernetines atakas, gelbsti valdant klimato kaitą. Paminėtinas Danijos pavyzdys, kai dirbtinio intelekto pagalba pavyksta efektyviau išsaugoti žmonių gyvybes, kai pagalbos tarnyba iš skambinančiojo balso gali nustatyti, kai sutrinka žmogaus širdies darbas (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018).

Dirbtinis intelektas vis labiau integruojamas į asmens gyvenimą. Šį teiginį patvirtina 2018 m. balandžio 25 d. Europos Sąjungos Komisijos komunikate „Dirbtinis intelektas Europai“ išdėstytas požiūris, kad dirbtinis intelektas yra daugelio gyvenimo dalis, o ne mokslinė fantastika (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018). Dėl šios technologijos plėtros, Europos Sąjunga siekia užtikrinti kuo didesnę naudą ir kuo mažesnę riziką vystant dirbtinį intelektą. Tai patvirtina Europos Sąjungos teisės aktų ir *soft law* šaltinių iniciatyvos. Pavyzdžiui, 2017 m. vykusiame Europos Vadovų Tarybos susitikime buvo išreikštas susirūpinimas, kad Europos Sąjunga turėtų skubiai reaguoti į besikeičiančias technologijas, apimančias dirbtinį intelektą bei kartu siekti užtikrinti aukštą duomenų apsaugos lygį (Europos Parlamento ir Tarybos Reglamentas Nr. 2021/694 kuriuo nustatoma Skaitmeninės Europos programa..., 2021). 2020 m. Europos Sąjungos Komisija Baltojoje knygoje „Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą“ (toliau – **Europos Sąjungos Komisijos Baltoji**

knyga) iškėlė dvejopą tikslą, t. y. skatinti dirbtinio intelekto naudojimą ir mažinti su šia technologija susijusias rizikas (Dirbtinis intelektas. Europos požiūris į..., 2020, p. 1-2). 2021 m. Europos Parlamentas rezoliucijoje pabrėžė tikslą tapti pasauline lydere dirbtinio intelekto plėtimo srityje, laikantis Europos Sąjungos vertybių, Europos Sąjungos pagrindinių teisių chartijoje įtvirtintų pagrindinių teisių, įskaitant, asmens duomenų apsaugą (Europos Parlamento rezoliucija „Europos skaitmeninės ateities kūrimas: kliūčių..., 2021). 2023 m. Europos Sąjungos deklaracijoje dėl skaitmeninio dešimtmečio skaitmeninių teisių ir principų, dar kartą buvo patvirtintas Europos Sąjungos tikslas spartinti technologijų raidą ir teisinio aiškumo poreikį, siekiant užtikrinti Europos Sąjungos puoselėjamų vertybių ir pagrindinių teisių taikymą technologijų aplinkoje. Pabrėžiama, kad technologijų raida neturėtų reikšti teisių regreso. Tai reiškia, kad vykdant technologijų transformaciją būtina laikytis pagrindinių teisių, įskaitant teisę asmens duomenų apsaugą (Europos deklaracija dėl skaitmenino dešimtmečio skaitmeninių teisių..., 2023). Akivaizdu, kad Europos Sąjunga siekia lyderystės tiek vystant dirbtinį intelektą, tiek užtikrinant asmens duomenų apsaugą. Vis dėlto, nėra aiškios reglamentavimo sistemos, privalomąją galią turinčių teisės aktų ar politinių įsipareigojimų, kurie galėtų aiškiai apibrėžti dirbtinio intelekto taikymo sritį ir pagrindinių teisių apsaugą (Specialusis komitetas dirbtinio intelekto skaitmeniniame..., 2022, p. 11).

Dirbtinio intelekto pažanga kelia iššūkių duomenų apsaugos srityje. Dirbtinio intelekto varomoji galia yra informacija, kuri apima asmens duomenis. Sparčiai vystantis technologijoms, sugeneruojamų asmens duomenų kiekis kiekvienais metais didėja. Teigiama, kad per penkerius metus daugelis duomenų bus saugomi ir tvarkomi ne duomenų centruose, bet išmaniuose prie tinklo jungiamuose objektuose (pvz., gamybiniuose robotuose ar automobiliuose) (Dirbtinis intelektas. Europos požiūris į..., 2020, p. 4). Dėl tokios informacijos tvarkymo dirbtiniam intelektui tiesiogiai yra taikomas 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 (Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens..., 2016) (toliau – **BDAR**). BDAR užtikrinami griežti duomenų apsaugos standartai, įskaitant BDAR principus. BDAR yra bendrasis teisės aktas, kuris leidžia naudoti dirbtinį intelektą suderintą su asmens duomenų apsauga, tačiau BDAR nepateikia konkrečių gairių ar nurodymų, kaip šį tikslą pasiekti. Atitinkamai, taikant dirbtinį intelektą, svarbu atsižvelgti į BDAR principus, jų taikymo ypatumus ir problematiką, nes nuo jų priklauso, kaip konkrečios BDAR normos bus

įgyvendintos teorijoje ir praktikoje Europos Sąjungos valstybėje narėje, siekiant užtikrinti asmens duomenų apsaugą.

Darbo tikslas. Šio darbo tikslas yra išnagrinėti, kokiu mastu ir kaip taikomi BDAR principai dirbtinio intelekto kontekste, ir kitas aktualias BDAR nuostatas, kurių taikymas nulemia BDAR principų taikymo sritį.

Darbo uždaviniai. Darbo tikslui įgyvendinimui yra keliami šie darbo uždaviniai:

1) atskleisti dirbtinio intelekto sampratą ir iššūkius, turinčius įtakos asmens duomenų apsaugai;
2) išnagrinėti dirbtinio intelekto teisinio reguliavimo šaltinius Europos Sąjungos asmens duomenų apsaugos aspektu;
3) įvertinti, kokia apimtimi BDAR yra taikomas dirbtiniam intelektui;
4) nustatyti, kokių iššūkių kyla ar gali kilti taikant BDAR įtvirtintus asmens duomenų tvarkymo principus ir dirbtinį intelektą.

Objektas. Šiame darbe nagrinėjamos pagrindinės BDAR principų nuostatos, taikomos dirbtiniam intelektui. Pirmiausia darbe analizuojamos BDAR nuostatos, kurios nulemia BDAR principų taikymo sritį. Šios teisės normos yra svarbios siekiant apibrėžti asmens duomenų sampratą, duomenų valdytoją ir tvarkytoją, duomenų subjektą, BDAR teritorinę taikymo sritį dirbtinio intelekto kontekste. Toliau darbe analizuojami BDAR principai siaurąją prasme (t. y. nagrinėjami su asmens duomenų tvarkymu susiję principai). Konkrečiai, remiantis BDAR 5 straipsniu atskleidžiami su asmens duomenų tvarkymu susijusių principų (t. y. teisėtumo, sąžiningumo ir skaidrumo, duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo, duomenų tikslumo, saugojimo trukmės apribojimo, vientisumo ir konfidencialumo ir atskaitomybės) samprata, taikymo ypatumai ir problematika, atsižvelgiant į dirbtinio intelekto kontekstą.

Tyrimo metodai. Darbo objektas yra analizuojamas pasitelkiant lingvistinį, sisteminį ir teleologinį metodus. Naudojant lingvistinį metodą, aiškinamos BDAR ir *soft law* šaltinių nuostatų formuluotės ir jų sudėtiniai elementai. Šis metodas padėjo išanalizuoti pagrindines sąvokas: asmens duomenys, duomenų valdytojas ir duomenų tvarkytojas, dirbtinis intelektas. Sisteminiu metodu BDAR principų nuostatos vertinamos neatsiejamai nuo visos BDAR sistemos, *soft law* šaltinių ir specialiosios literatūros. Šiuo metodu buvo išskirti

svarbiausi šaltinių teiginiai ir pateiktos apibendrintos išvados. Pasitelkiant teleologinį metodą, siekiama atskleisti Europos Sąjungos įstatymų leidėjo siekiamą tikslą priimant konkrečią BDAR teisės normą.

Darbo originalumas. Užsienio doktrinoje panašia tema daugiausia pateikta mokslinių tyrimų ataskaitų, gairių ar atskirų monografijų. Pavyzdžiui, 2018 m. Norvegijos duomenų apsaugos tarnyba išleido ataskaitą „Artificial intelligence and privacy“ (Artificial intelligence and privacy, 2018), kurioje tiriamas sąžiningumo, skaidrumo, tikslo apribojimo ir duomenų mažinimo principai dirbtinio intelekto kontekste. 2020 m. Ispanijos duomenų apsaugos agentūra paskelbė gaires „GDPR compliance of processings that embed Artificial Intelligence An introduction“, kuriose analizuojami teisėto duomenų tvarkymo pagrindai ir duomenų subjektų teisės dirbtinio intelekto kontekste. 2020 m. Europos Parlamento tyrimų tarnyba paskelbė publikaciją „The impact of the General Data Protection Regulation (GDPR) on artificial intelligence“ ir publikacijos priedą „The impact of the General Data Protection Regulation (GDPR) on artificial intelligence“, kuriose tiriamas BDAR taikymas dirbtiniam intelektui. Konkrečiai, publikacijoje ir jos priede yra analizuojamas dirbtinis intelektas ir asmens duomenų apsauga, profiliavimas, sutikimas, duomenų apsaugos principai, duomenų subjektų teisės ir automatinis sprendimų priėmimas.

Lietuvoje, autorės žiniomis, panaši tema buvo nagrinėjama magistro darbuose: 2018 m. A. Aiduko „Data Privacy and Artificial Intelligence: Is General Data Protection Regulation the Right Regulation in the Age of Intelligent Machines?“, 2018 m. A. Babayan „Dirbtinio intelekto iššūkis žmogaus teisių apsaugos sričiai: robotų statuso reguliavimas“, 2020 m. A. Kabašinskaitės „ES Bendrojo duomenų apsaugos reglamento vaidmuo ketvirtojoje pramonės revoliucijoje“, 2020 m. K. Seliulaitės „ES Bendrojo duomenų apsaugos reglamento taikymo dirbtiniam intelektui ypatumai“.

Šis magistro darbas išsiskiria BDAR reguliavimo tyrimo apimtimi ir atsirandančiu nauju požiūriu dėl dirbtinio intelekto plėtojimo Europos Sąjungoje. Darbo tyrimo apimtis yra BDAR principai, t. y. daugelis kitų darbų buvo parengti analizuojant plačia apimti BDAR ir dirbtinį intelektą. Tuo tarpu, šiame magistro darbe dirbtinio intelekto problematika yra analizuojama BDAR principų prasme. Atitinkamai, tai lemia ir skirtingos apimties darbo objektą, analizuojamas problemas ir pateiktas išvadas. Magistro darbas parengtas remiantis naujausiais moksliniais straipsniais ir Europos Sąjungos *soft law* šaltiniais dėl dirbtinio intelekto teisinio reguliavimo, apimant 2021 m. balandžio 21 d. Europos Sąjungos Komisijos pasiūlymą „Europos Palamento ir Tarybos reglamentas,

kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai) (Europos Komisijos pasiūlymas Europos Parlamento ir Tarybos Reglamentas kuriuo nustatomas suderintos dirbtino intelekto..., 2021) (toliau – **Dirbtinio intelekto aktas**), kuriuo siekiama reguliuoti didelės rizikos dirbtinio intelekto sistemas. Dėl Dirbtinio intelekto akto Europos Sąjungos Parlamentas turėtų balsuoti iki 2023 m. kovo pabaigos, o po šio balsavimo balandžio mėnesį turėtų prasidėti trišalis dialogas tarp valstybių narių, Europos Sąjungos Parlamento ir Europos Sąjungos Komisijos. Jei bus laikomasi šio grafiko, Dirbtinio intelekto aktas turėtų būti priimtas iki 2023 m. pabaigos (Drake *et al.*, 2023).

Svarbiausi šaltiniai. Pagrindiniai šio darbo tyrimo šaltiniai yra BDAR ir priimti Europos Sąjungos institucijų *soft law* teisės aktais. Buvo remtasi užsienio ir Lietuvos teisės mokslininkų darbais: C. Kuner, L. A. Bygrave, C. Docksey „The EU General Data Protection Regulation. A Commentary (Kuner *et al.*, 2020), „The EU General Data Protection Regulation: A Commentary Update of Selected Articles (Kuner *et al.*, 2021) F. Marengo „Data protection law in charts“ (Marengo, 2021), J. Zaleskio „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“ (Zaleskis, 2019). Taip pat, šiame darbe buvo remiamasi Europos duomenų apsaugos valdybos gairėmis, Europos Sąjungos Duomenų apsaugos direktyvos 29 straipsniu įsteigtos Darbo grupės (toliau – **29 straipsnio duomenų apsaugos darbo grupė**) nuomonėmis, Specialaus dirbtinio intelekto skaitmeniniame amžiuje komiteto ir Aukšto lygio ekspertų grupės dirbtinio intelekto klausimais ataskaitomis bei Europos Sąjungos Teisingumo Teismo praktika. Autorės nuomone, svarbiausi šaltiniai tyrimui buvo Europos Sąjungos institucijų *soft law* teisės šaltiniai: Europos duomenų apsaugos valdybos gairės, Europos Sąjungos 29 straipsnio darbo grupės nuomonės ir Europos Parlamento mokslinių tyrimų tarnybos ataskaita, nes dalis minėtų šaltinių (pvz., Europos duomenų apsaugos valdybos gairės) pateikė sistemingą požiūrį į praktinius BDAR principų reguliavimo aspektus, kiti minėti šaltiniai (pvz., *soft law* teisės aktai, Europos Parlamento mokslinių tyrimų tarnybos ataskaita) išdėstė reikšmingą Europos Sąjungos požiūrį į dirbtinio intelekto reguliavimą. Taip pat, aktualus Dirbtinio intelekto aktas, įtvirtinantis dirbtinio intelekto sistemų apibrėžimą ir reglamentuojantis dirbtinio intelektų sistemų teisėtą naudojimą.

1. DIRBTINIS INTELEKTAS IR JO TEISINIO REGULIAVIMO SISTEMA

1.1. Dirbtinio intelekto samprata

Tiksli dirbtinio intelekto sampratos apibrėžtis dinamiškuose skaitmeninių technologijų srityse yra iššūkis. Tai reiškia, kad dirbtinis intelektas vis dar yra neapibrėžta sąvoka, dėl kurios apibrėžties nėra susitarimo nei techniniu, nei teisiniu ar politiniu lygmeniu. Per keletą dešimtmečių buvo bandoma pateikti įvairių dirbtinio intelekto sampratų. Tačiau sparti technologijų pažanga ir atsirandančių naujų sąvokų suvokimas (pvz., mašininis mokymasis (angl. *machine learning*) arba gilusis mokymasis (angl. *deep learning*)), vis dar kelia neaiškumo (Berryhill *et al.*, 2019, p. 30). Pastebima, kad dirbtinio intelekto apibrėžčių yra daugybė, tačiau neretai šios apibrėžtys yra itin plačios arba pernelyg specifinės ir pritaikytos konkrečiam sektoriui (Artificial intelligence and privacy, 2018, p. 5). Be to, pripažįstama, kad dirbtinio intelekto apibrėžties kūrimas yra nuolatinis procesas, kuriuo metu atsižvelgiama į dirbtinio intelekto kontekstą ir į visuomenės pokyčius šioje srityje (Europos regionų komiteto nuomonė „Europos požiūris į dirbtinį intelektą..., 2020). Esant dirbtinio intelekto apibrėžties problematikai yra suduriama su teisiniu neaiškumu, kadangi bet kokiame teisiniame akte dirbtinio intelekto apibrėžtis turės būti pakankamai lanksti, kad būtų galima atsižvelgti į technologijų pažangą, tačiau ir tiksli, kad būtų užtikrintas būtinas teisinis tikrumas (Dirbtinis intelektas. Europos požiūris į..., 2020, p. 17).

Europos Sąjunga siekdama reguliuoti dirbtinį intelektą, ėmėsi iniciatyvos pateikiant dirbtinio intelekto apibūdinimą. 2018 m. balandžio 25 d. Europos Sąjungos Komisija komunikate „Dirbtinis intelektas Europai“ nurodė, kad dirbtinis intelektas yra „sistemos, kurios elgiasi protingai, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti“ (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018). Vis dėlto, Europos Sąjungos Komisijos įsteigta Aukšto lygo ekspertų grupė dirbtinio intelekto klausimais (Europos Komisijos Komunikatas Pasitikėjimo į žmogų orientuotu dirbtiniu..., 2019) pasiūlė išplėsti Europos Sąjungos Komisijos siūlytą dirbtinio intelekto apibrėžtį, nurodydama, kad dirbtinis intelektas turėtų būti suprantamas kaip dirbtinio intelekto sistemos, kurios yra žmonių sukurtos programinės įrangos, kurioms nustačius tikslą, veikia fiziniu ir skaitmeniniu lygiu – analizuoja savo aplinką rinkdamos duomenis, aiškina duomenis, analizuoja turimas žinias ir priima sprendimą, kuris geriausia atitinka siekiamą tikslą (Aukšto lygio ekspertų grupė dirbtinio..., 2019a, p. 6). Minėtas apibrėžimas yra įtvirtintas Dirbtinio intelekto akto 3 straipsnio 1 dalyje, kuriuo nustatoma, kad dirbtinio intelekto sistema yra programinė įranga, sukurta taikant vieną ar daugiau Dirbtinio intelekto akto I priede išvardytų metodų ir gebanti pagal tam tikrus žmogaus nustatytus

tikslus generuoti išvedinius (pvz., turinį, predikcijas, rekomendacijas, arba sprendimus, turinčius įtakos aplinkai, su kuria ji sąveikauja). Pagal Dirbtinio intelekto akto I priedo a-c punktus, dirbtinio intelekto sistema turi būti sukurta remiantis mašininiu mokymosi (įskaitant gilųjį mokymąsi), logika ir žiniomis pagrįstais pagrindais bei statistiniais metodais. Atkreiptinas dėmesys, kad Dirbtinio intelekto akto 4 straipsniu suteikiami Europos Sąjungos Komisijai įgaliojimai priimti deleguotuosius aktus, kuriais būtų keičiami Dirbtinio intelekto akto I priede nurodytų metodų sąrašas siekiant jį pritaikyti prie rinkos ir technologijų pokyčių. Tai reiškia, kad dirbtinio intelekto apibrėžimas laikui bėgant turi keistis atsižvelgiant į dirbtinio intelekto sistemų ir prietaisų pažangą (Europos regionų komiteto nuomonė „Europos požiūris į dirbtinį intelektą..., 2022).

Nepaisant dirbtino intelekto apibrėžties problematikos, yra sutariama, kad dirbtinis intelektas yra neatsiejamas nuo dirbtinio intelekto komponentų. Šiandien vyraujantys dirbtinio intelekto komponentai yra mašininis ir gilusis mokymasis. Nors mašininis mokymasis ir dirbtinis intelektas neretai vartojami kaip sinonimai, mašininis mokymasis tiksliau turėtų būti suprantamas kaip vienas iš dirbtinio intelekto kūrimo būdų (Mitrou, 2018, p. 12). Mašininis mokymasis apibrėžiamas kaip dirbtinio intelekto posistemė, kuri automatiškai mokosi ir tobulėja iš anksčiau įvestų veiksmų rinkinių (Kanade, 2022). Dauguma mašininio mokymosi metodų veikia aptikdami naudingus dėsningumus dideliuose duomenų kiekiuose (What Is Machine Learning? How..., 2023). Tradiciškai mašininis mokymasis gali atlikti sudėtingas dirbtinio intelekto užduotis (pvz., vaizdų atpažinimą) ir analizuoti besikeičiančius informacijos srautus (Leong *et al.*, 2020, p. 5) Naudojant mašininio mokymosi sistemą Japonijoje buvo sukurtas krepšinį žaidžiantis robotas „CEU“, kuris meta baudas 100 proc. tikslumu. Roboto taiklumas yra žymiai tikslesnis nei NBA krepšininkų vidurkis, kuris yra 77 proc. (Campanaro, 2018). Tuo tarpu, gilusis mokymasis yra mašininio mokymosi poaibis, kuris mokosi apdorodamas duomenis dirbtinių neuronų tinklų pagalba (Kanade, 2022), siekdamas imituoti žmogaus sprendimų priėmimą (Artificial Intelligence and Data Protection..., 2018, p. 7). Tai reiškia, kad gilusis mokymasis naudoja daugybę dirbtinių neuronų tinklų, tokiu būdu siekdamas imituoti žmogaus sprendimų priėmimą. Ši technologija yra daugelio šiandien kuriamų dirbtinio intelekto programų pagrindas ir ji įgalina tokias technologijas, kaip kompiuterinis matymas, teksto klasifikavimas, modelių atpažinimas, kalbos supratimas, prognozavimas ar rekomendavimas (Kanade, 2022). Dėka gilaus mokymosi, dirbtinis intelektas gali atpažinti objektus nuotraukose, įvertinti spalvų vertes ir dažniausiai kitus su turimu duomeniu susijusius objektus, kad dirbtinio intelekto naudotojui būtų galima pateikti išvestines prognozes (Leong *et al.*, 2020, p. 17). Giliojo mokymosi pavyzdys yra 2022 m.

lapkričio mėn. sukurtas ChatGPT, kurio pagrindinė funkcija yra imituoti žmogaus pokalbį. Be šios funkcijos, ChatGPT gali kurti kompiuterines programas, rašyti dainų tekstus, atsakinėti į testų klausimus ar net rašyti mokslinius tekstus (AI is finally good at..., 2020). ChatGPT naudoja didelius duomenų kiekius, kad suprastų kontekstą, tinkamumą ir priimtų sprendimą, kaip generuoti atsakymus (ChatGPT: What Is It and..., 2023).

Atsižvelgiant į tai, kas bus išdėstyta, darytina išvada, kad visuotinai pripažinto dirbtinio intelekto apibrėžimo vis dar nėra. Europos Sąjungos Komisija siekdama reguliuoti dirbtinį intelektą, pateikė pasiūlymą dėl dirbtinio intelekto apibrėžties, tačiau Dirbtinio intelekto teisės aktas vis dar nėra priimtas ir įtvirtintas dirbtinio intelekto apibrėžimas nėra pripažintas oficialiu Europos Sąjungos lygiu. Turint omenyje tai, kad bet koks reguliavimas turi atsakyti į klausimą, kas yra reguliuojama, šiame darbe dirbtinio intelekto apibrėžtis bus pripažįstama dirbtinio intelekto bendriniu suvokimu, dirbtinį intelektą aiškinant kaip sistemas, kurios pasižymi protingu „kognityviniu“ elgesiu analizuojančiu savo aplinką ir galinčiu priimti gana savarankiškus sprendimus tikslui pasiekti (Lietuvos dirbtinio intelekto strategija. Ateities..., 2020, p. 5).

1.1.1. Dirbtinis intelektas ir algoritmai

Algoritmai apibrėžiami kaip baigtinės ir vienareikšmės veiksmų sekos, kurios yra skirtos pasiekti rezultatą iš pradinių įvestų duomenų (t. y. didžiulio kiekio asmens arba ne asmens duomenų) (Demiaux *et al.*, 2017, p. 15). Tai reiškia, kad (1) kiekvienas algoritmo etapas turi būti atskiras ir kiekvienu etapu turi būti siekiama viena išvada; (2) algoritmui įvesti duomenys turi būti tikslūs ir aiškiai apibrėžti; (3) algoritme turi būti aiškiai nurodytas rezultatas, kuris turi būti pasiektas (What is Algorithm? Definiton of..., 2023). Algoritmai gali būti paprasti (pvz., nurodantys, kaip surasti didžiausią dviejų skaičių daliklį) arba sudėtingi (pvz., nurodantys kalbų atpažinimą ar finansines prognozes) (The impact of the General..., 2020a, p. 3). Neretai algoritmas yra lyginamas su receptu, kurį sudaro konkretūs veiksmai, kurie nurodo, kaip pasiekti norimą rezultatą (Downey *et al.*, 2020). Kasdienybėje algoritmai leidžia pasiekti įvairius rezultatus: rekomenduoti klientams knygas pagal kitų klientų jau padarytus pasirinkimus, atlikti skaitmeninę veidų ar pirštų atspaudų lyginimą (Demiaux *et al.*, 2017, p. 15).

Dirbtinis intelektas imituodamas „kognityvines“ funkcijas, naudoja algoritmus, siekdamas priimti automatizuotus sprendimus (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 363). Tačiau algoritmai yra bendresnis terminas negu dirbtinis intelektas (Russell *et al.*, 2016, p. 27). Tai reiškia tam, kad algoritmai galėtų veikti jie

privalo būti išreikšti programavimo kalbomis ir tapti mašininio mokymosi programomis (The impact of the General..., 2020a, p. 3). Dirbtinį intelektą galima traktuoti kaip sudėtingą algoritmą, kuris jungia įvairias jo funkcijas atliekančius algoritmus. Vis dėlto, dirbtinis intelektas gali mokytis, todėl jo svarbiausias komponentas yra ne išmoktų algoritmų veiksmų seka, o mokymosi algoritmai, kurie keičia algoritmo veiksmų seką, siekdami atlikti savo funkciją (The impact of the General..., 2020a, p. 4).

Vadinasi, dirbtinis intelektas yra grindžiamas algoritmais, kuriems reikia įvestų duomenų, kad algoritmas galėtų atlikti siekiamą tikslą.

1.1.2. Dirbtinis intelektas ir didieji duomenys

Didieji duomenys (angl. *big data*) apibrėžiami kaip sudėtingas ir didelės apimties informacijos rinkinys, susidedantis iš duomenų rinkinių, kuriuos sudėtinga tvarkyti naudojant tradicines duomenų apdorojimo priemones (Guidelines on the protection of..., 2017, p. 2). Tai reiškia, kad didieji duomens yra duomenų kiekiai, kurių apimtis yra milžiniškos ir kurie nuolat, ir sparčiai didėja (BasuMallick, 2020). Didžiųjų duomenų savybės atskleidžiamos per tris didžiųjų duomenų aspektus (angl. *„Three V's"*) (What Is Big Data?, 2023): (1) apimtį (angl. *volume*), kuri reiškia, kad šiandien sukuriama ir saugoma daug duomenų; (2) greitį (angl. *velocity*), reiškiantį, kad duomenys yra generuojami didesniu greičiu nei bet kada anksčiau; (3) įvairovę (angl. *varienty*), kuri suponuoja, kad duomenys yra įvairių formų ir pavidalų (pvz., teksto, vaizdo ar garso įrašai) (Berryhill et al., 2019, p. 21). Didžiųjų duomenų šaltinių yra įvairių. Didieji duomenys apima informaciją apie žmones, jų duomenis, įrenginius ar jutiklius, informaciją apie klimatą, palydovų užfiksuotus atvaizdus, skaitmenines nuotraukas, vaizdo medžiagą ar GPS signalus. Pastebima, kad didžiųjų duomenų informacijos dalis yra asmens duomenys (pvz., vardas, pavardė, nuotrauka, el. pašto adresas, banko duomenys, GPS sekimo duomenys, socialinių tinklų interneto svetainių adresai, medicininė informacija ar kompiuterio IP adresas) (Europos Komisijos faktų apie duomenų...., 2017 cituota Europos Sąjungos pagrindinių teisių agentūra, 2018, p. 362). Didžiuosius duomenis gali kurti žmonės, tačiau neretai jie renkami naudojant mašinas, kurios fiksuoja informaciją erdvėje (pvz., gatvių kameros) arba iš kompiuterių veiklos (pvz., internetinės svetainės, kurios stebi elgseną internete) (The impact of the General..., 2020a, p. 4). Didieji duomenys teikia informaciją apie asmenis, siekiant privačioms įmonėms vystyti rinkodarą, reklamą ar siūlomas akcijas. Taip pat, naudojami medicinos tikslais, siekiant nustatyti ligų požymius ir rizikos veiksnius ar diagnozuoti sveikatos sutrikimus. Be to, derinant duomenis iš įvairių

sveikatos, žiniasklaidos, interneto svetainių, gali būti suteikiama informacija apie infekcinių ligų protrūkius (Botelho *et al.,* 2022).

Ryšys tarp dirbtinio intelekto ir didžiųjų duomenų yra abipusis. Tai reiškia, kad dirbtiniam intelektui reikia duomenų, kad jis galėtų mokytis. Tuo tarpu, didieji duomenys naudoja dirbtinį intelektą, kad išgautų duomenis iš duomenų rinkinių (Artificial Intelligence, Robotics, Privacy and..., 2016, p. 4). Dirbtinis intelektas remiasi dideliais duomenis, kad sukurtų tikslius modelius siekiamoms užduotims atlikti (Eager *et al.,* 2020, p. 15).

Taigi, didieji duomenys yra viena iš pagrindinių dirbtinio intelekto varomųjų jėgų. Dirbtiniam intelektui reikalingi duomenys, o šis poreikis yra užtikrinamas dirbtiniam intelektui padedant duomenis išgauti iš duomenų rinkinių ir tokiu būdu kuriant didžiuosius duomenis.

1.1.3. Dirbtinis intelektas ir robotika

Robotika yra fizikos, inžinerijos ir skaitmeninių technologijų sankirtoje esantis sritis, kurioje yra kuriamos mašinos, galinčios pakeisti, papildyti ar atkartoti fizinio asmens veiksmus (Leong *et al.*, 2020, p. 13). Robotą sudaro trys pagrindiniai veiksniai: (1) robotai sąveikauja su fiziniu pasauliu per jutiklius; (2) robotai yra programuojami; (3) robotai yra autonomiški arba pusiau autonomiški (Ziyad, 2018/2019, p. 3). Šiandien robotai naudojami skirtingoms funkcijoms. Robotai veikia saugumo (pvz., užminuotų prietaisų šalinime iš pavojingos zonos), karybos (pvz., karinių krovinių pernešime), mokslo (pvz., tiesiant zondus, kurie siunčiamai į kosmosą ar pavojingą aplinką (pvz., gilumines vandenyno vietas) (Artificial Intelligence, Robotics, Privacy and..., 2016, p. 20) ar kasdienio gyvenimo (pvz., robotai dulkių siurbliai) (Aukšto lygio ekspertų grupė dirbtinio..., 2019a, p. 4) srityse.

Šiuo metu daugelis robotų nėra dirbtinis intelektas. Neretai robotai yra užprogramuoti atlikti tik pasikartojančius judesius, o pasikartojantiems judesiams dirbtinio intelekto nereikia (Ziyad, 2019, p. 3). Nors robotika nėra kelias į dirbtinį intelektą, tačiau įvairių formų robotai įgauna vis daugiau intelektinių gebėjimų, kuriuos lemia nuolatinis juos valdančių dirbtinio intelekto sistemų tobulėjimas (Leong *et al.*, 2020, p. 13). Vis dėlto, Europoje ima vyrauti suvokimas, kad robotiką galima apibrėžti ir kaip dirbtinio intelekto veikimą fiziniame pasaulyje. Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais nurodė, kad robotas yra fizinė mašina, kuri yra paremta suvokimu, logine analize ir mokymosi sąveika su kitomis sistemomis (Aukšto lygio ekspertų grupė dirbtinio..., 2019a, p. 4)

Taigi, nors vis dar nėra vieno pripažinto standarto, ar dirbtinis intelektas yra robotikos dalis, vis dėlto, klesti suvokimas, kad dirbtinis intelektas gali būti robotikos pagrindas, kurio tikslas yra sukurti mašinas, kurios galėtų priimti sprendimus erdvėje.

1.2. Dirbtinio intelekto iššūkiai ir jų sąsaja su duomenų apsauga

Dirbtinio intelekto klestėjimas suteikia dinamiškų galimybių prisidėti prie valdžios institucijų veiklos efektyvumo, privačių įmonių produktyvumo ar kasdienių asmenų užduočių atlikimo. Nekvestionuojama, kad šiuo metu dirbtinis intelektas yra pasiekęs aukštą perspektyvos lygį ir juo vaidmuo svarbus tiek pramonės, tiek sveikatos priežiūros, tiek daugelyje kitų sričių (Galindo *et al.*, 2021, p. 5). Vis dėlto, šiuo metu teisinės sistemos susiduria su precedento neturinčiais su dirbtiniu intelektu susijusiais iššūkiais (Artificial Intelligence ante portas: Legal..., 2019, p. 1).

Kuriant ir naudojant dirbtinį intelektą daugeliu atvejų yra tvarkomi asmens duomenys. Dirbtinis intelektas yra neatsiejamas nuo didelių kiekių asmens duomenų tvarkymo (Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos, 2019). Mokslinėse publikacijose pabrėžiama, kad dirbtinis intelektas yra „alkanas asmens duomenų“ (Paal, 2022, p. 290). Todėl siekiant užtikrinti tinkamą dirbtinio intelekto veikimą, dirbtinis intelektas reikalauja prieigos prie didelės apimties asmens duomenų, įskaitant fizinio asmens rasę, etninę kilmę, lytį ar kitus neskelbtinus duomenis (Artificial Intelligence *ante portas*: Legal..., 2019, p. 3). Asmens duomenys dirbtiniam intelektui yra svarbūs, nes kuo daugiau informacijos dirbtinis intelektas surenka, tuo geriau jis gali suvokti ir aptikti duomenų ryšius, ir priimti sprendimus (Europos Komisijos Komunikatas Suderintas dirbtinio intelekto planas, 2018). Vis dėlto, dėl tokio didelio asmens duomenų kiekio rinkimo kyla iššūkių, susijusių su dirbtinio intelekto renkamų duomenų kiekiu, dirbtinio intelekto šališkumu, poreikiu užtikrinti žmogiškąją veikimo kontrole ir šių intelektualių sistemų atsakomybę (Artificial Intelligence ante portas: Legal..., 2019, p. 3). Atitinkamai, naudojant dirbtinį intelektą, kyla poreikis užtikrinti, kurį išreiškė ir Europos Sąjungos Komisija Baltojoje knygoje, kad dirbtinis intelektas turi būti grindžiamas Europos Sąjungos vertybėmis ir pagrindinėmis teisėmis, įskaitant teisę į asmens duomenų apsaugą (Dirbtinis intelektas. Europos požiūris į..., 2020, p. 2).

Europos Sąjungos sutarties 2 straipsnyje nustatytos Europos Sąjungos vertybės: „<...> pagarba žmogaus orumui, laisve, demokratija, lygybe, teisine valstybe ir pagarba žmogaus teisėms, įskaitant mažumoms priklausančių asmenų teises <...>“ (Europos Sąjungos sutartis, 2008). Siekiant stiprinti pagrindinių teisių apsaugą, Europos Sąjungos

pagrindinių teisių chartijoje yra pripažįstamos pagrindinės Europos Sąjungos teisės, laisvės ir principai (Europos Sąjungos pagrindinių teisų chartija, 2016). Europos Sąjungos pagrindinių teisių chartijos 8 straipsnis nustato, kad kiekvienas asmuo turi teisę į duomenų apsaugą. Sutarties dėl Europos Sąjungos veikimo 16 straipsnio 1 dalyje įtvirtinama kiekvieno asmens teisė į asmens duomenų apsaugą (Sutartis dėl Europos Sąjungos veikimo, 2012).

Teisės į asmens duomenų apsaugą užtikrinimas yra svarbus kuriant ir priimant dirbtinio intelekto sprendimus, kurie gali turėti pasekmių asmenims (Artificial intelligence and data protection, 2019, p. 7). Dirbtinis intelektas tvarko asmens duomenis, todėl duomenų apsaugos teisė gali būti pažeidžiama, kai dirbtinio intelekto vykdomos funkcijos turi trūkumų. Visų pirma, Europos Sąjungos gerojoje praktikoje akcentuojamas iššūkis kylantis dėl to, kad dirbtinis intelektas gali naudoti neobjektyvius duomenis (pvz., dirbtinis intelektas gali būti apmokytas daugiau moterų duomenimis, todėl vyrų atžvilgu gali būti gaunami netikslūs rezultatai) (Dirbtinis intelektas. Europos požiūris į..., 2020, p. 11). Antra, dirbtinis intelektas gali tvarkyti asmens duomenis nesirenkant ir neproporcingai dideliais kiekiais vien tik siekdamas nustatyti tik kelių asmenų tapatybę (pvz., keleivių oro uostuose). Dėl tokio duomenų tvarkymo kyla skaidrumo problemų ir klausimų, susijusių ir su asmens duomenų tvarkymo teisiniu pagrindu (Europos duomenų apsaugos valdyba *et al.,* 2021, p. 12). Trečia, kaip buvo minėta, dirbtinis intelektas renka didelius asmens duomenų kiekius (Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos..., 2019), todėl išlieka neaišku, kaip dirbtinio intelekto kūrėjai ar naudotojai turėtų užtikrinti tinkamą galimybę fiziniams asmenims susipažinti su surinktais duomenimis, kontroliuoti juos ar net reikalauti, kad duomenys toliau nebūtų tvarkomi (Artificial intelligence and data protection, 2019, p. 10). Galiausiai, Europos duomenų apsaugos priežiūros pareigūnas yra nurodęs, kad kyla rizika, susijusi su naudojimosi dirbtiniu intelektu, kai žmogus pernelyg pasitiki dirbtinio intelekto sprendimų priėmimu (Europos duomenų apsaugos priežiūros pareigūnas, 2020, p. 10). Pabrėžiama, kad dirbtinio intelekto sprendimų priėmimas gali būti netikslus dėl šališkų, netinkamos kokybės duomenų ar dėl įgytų dirbtinio intelekto projektavimo aspektų, kurių dirbtinio intelekto kūrėjai ar naudotojai gali nekontroliuoti (Leong *et al.,* 2021, p. 6-7).

Remiantis išdėstyta informacija, daryti išvada, kad fizinių asmenų apsauga tvarkant jų asmens duomenis yra pagrindinė teisė. Teisė į asmens duomenų apsaugą dirbtinio intelekto kontekste nėra užtikrinama pilna apimtimi, nes dirbtinis intelektas remiasi didžiuliai asmens duomenų kiekiai, kurie kelia iššūkius susijusių asmens duomenų

objektyvumu, perteklinių asmens duomenų rinkimu, dėl kurių fiziniai asmenys tinkamai negali kontroliuoti tvarkomų asmens duomenų ir priimamų dirbtinio intelekto sprendimų.

1.3. Asmens duomenų apsaugos dirbtiniame intelekte teisės šaltiniai

Kaip buvo minėta, dirbtinio intelekto naudojimas gali kelti iššūkių susijusių su asmens teisę į duomenų apsaugą. Kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą, taikomos duomenų apsaugą reguliuojančios teisės normos. Atitinkamai, šiame skyriuje bus aptariami svarbiausi asmens duomenų apsaugos teisės šaltiniai ir dirbtinį intelektą reguliuojantys Europos Sąjungos teisės normos, ir *soft law* šaltiniai.

Duomenų apsaugos teisės šaltinius yra galima skirstyti į pirminius ir antrinis. Pirminiai šaltiniai nustato duomenų subjektų teises (pvz., duomenų apsaugos norminiai aktai, bendrieji teisės principai, teismų praktika). Antriniuose šaltiniuose atskleidžiamas pirminiuose šaltiniuose įtvirtintų teisės normų taikymas ir aiškinimas (pvz., *soft law* ir teisės doktrina). Be to, duomenų apsaugos teisės šaltiniai gali būti skirstomi pagal teisinę sistemą: tarptautinės teisės, Europos Sąjungos teisės ir Lietuvos Respublikos nacionalinės teisės (Zaleskis, 2019, p. 60).

Tarptautiniai duomenų apsaugos teisės šaltiniai yra išskirti Tarptautinio Teisingumo Teismo Statuto 38 straipsnio 1 dalies a-d punktuose, nustatančiuose, kad tarptautinius teisės šaltinius sudaro tarptautinės konvencijos, tarptautinis paprotys, bendrieji teisės principai ir teisės doktrina (Tarptautinio Teismo Statutas, 1945). Atitinkamai, duomenų apsaugos teisės šaltiniai yra tarptautinės sutartys, pavyzdžiu, Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija (Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, 1950) ir Tarptautinis pilietinių ir politinių teisių paktas (Tarptautinis pilietinių ir politinių teisų paktas, 1966) (Zaleskis, 2019, p. 61). Nors minėtos tarptautinės sutartys nereglamentuoja teisės į duomenų apsaugą, tačiau yra pripažįstama teisė į privatumą, kuri yra aktuali asmens duomenų tvarkymui naudojant dirbtinį intelektą. Kitas Europos Tarybos tarptautinis teisės aktas – Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis (Konvencija dėl asmenų apsaugos ryšium..., 1981) (toliau – **Europos Tarybos duomenų apsaugos konvencija**), kuri yra aktuali dirbtinio intelekto kontekste. Asmens duomenys pasitelkiant dirbtinį intelektą yra tvarkomi automatizuotu būdu, todėl dirbtinis intelektas patenka į minėto teisės akto taikymo sritį ir yra svarbus tarptautiniu lygiu taikomas duomenų apsaugos teisės šaltinis.

Europos Sąjungos teisės šaltinius sudaro Europos Sąjungos pirminė teisė (t. y. Europos Sąjungos sutartis, Sutartis dėl Europos Sąjungos veikimo, Europos Sąjungos pagrindinių teisių chartija, Europos atominės energijos bendrijos steigimo sutartis (Europos atominės energijos bendrijos steigimo..., 2016) ir antrinė teisė (t. y. reglamentai, direktyvos, sprendimai, rekomendacijos ir nuomonės) (Sutarties dėl Europos Sąjungos veikimo 288 straipsnis). Duomenų apsaugos teisės kontekste, pirminis teisės šaltinis yra Europos Sąjungos pagrindinių teisių chartija ir Sutartis dėl Europos Sąjungos veikimo, kurios nustato kiekvieno asmens teisę į duomenų apsaugą. Antrinis Europos Sąjungos teisės šaltinis yra BDAR. Europos Sąjunga visada laikėsi griežto požiūrio į asmens duomenų apsaugą. Dar 1995 m. Europos Sąjunga priėmė Europos Parlamento ir Tarybos direktyva dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo anksčiau, nei asmenų duomenys tapo aktualūs internete (Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens..., 1995). Vėliau buvo priimtas BDAR, kuriuo siekiama suderinti visų valstybių narių duomenų apsaugos įstatymus, apsaugoti asmens duomenų perdavimą į trečiąsias šalis ir suteikti duomenų subjektams teisę kontroliuoti savo asmens duomenis. BDAR aktualus dirbtiniam intelektui, nes (1) BDAR 2 straipsnyje nustatyta, kad BDAR taikomas, kai tvarkomi asmens duomenys. Buvo minėta, kad dirbtinis intelektas yra pagrįstas informacija, kurią sudaro ir asmens duomenys; (2) BDAR 22 straipsnyje reglamentuojamas automatizuotų sprendimų priėmimas, įskaitant profiliavimą. Dirbtiniu intelektu asmens duomenys yra tvarkomi automatizuotu būdu, todėl akivaizdu, kad BDAR poveikis dirbtinio intelekto plėtrai yra neišvengiamas (How to Train an AI..., 2022). Be to, BDAR yra technologiškai neutralus teisės aktas ir nepriklauso nuo duomenų tvarkymo metodų (Zaleskis, 2019, p. 322), todėl taikomas visoms informacinėms technologijoms, įskaitant ir dirbtinį intelektą. Atkreiptinas dėmesys, kad BDAR sudaro BDAR principai, kurie yra pagrindas visam BDAR rėžimui ir su kurių taikymo iššūkiais susiduria dirbtinis intelektas. Be BDAR, dirbtiniam intelektui yra taikomi kiti antriniai Europos Sąjungos teisės aktai (pvz., Europos Parlamento ir Tarybos direktyva dėl mašinų, iš dalies keičianti Direktyvą Nr. 95/16/EB (Europos Parlamento ir Tarybos direktyva dėl mašinų, iš dalies keičianti..., 2006), Tarybos Direktyva dėl valstybių narių įstatymų ir kitų teisės aktų, reglamentuojančių atsakomybę už gaminius su trūkumais, derinimo (Tarybos direktyva dėl valstybių narių įstatymų ir..., 1985), Europos Parlamento ir Tarybos reglamentas dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų (Europos Parlamento ir Tarybos reglamentas dėl ne asmens duomenų judėjimo..., 2018). Tačiau minėti aktai šiame darbe nebus nagrinėjami detaliau, nes nepatenka į darbo objekto apimtį.

Lietuvos Respublikos nacionalinius teisės šaltinius sudaro tarptautinės sutartys, Europos Sąjungos teisės aktai, bendrieji tarptautinės teisės principai, teismų praktika ir teisės doktrina. Aukščiausią galią turintis teisės aktas yra Lietuvos Respublikos Konstitucija, kurioje įtvirtintas privataus gyvenimo neliečiamumas (Zaleskis, 2019 p. 61). Lietuvos Respublikoje galioja Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, 2018) (toliau – **Asmens duomenų apsaugos įstatymas**), kuriuo siekiama saugoti žmogaus pagrindines teises ir laisves, visų pirma, žmogaus teisę į asmens duomenų apsaugą, ir užtikrinti aukštą asmens duomenų apsaugos lygį (Lietuvos Respublikos duomenų teisinės apsaugos įstatymo 1 straipsnio 1 dalis). Asmens duomenų apsaugos įstatymas aktualus asmens duomenų tvarkymui pasitelkiant dirbtinį intelektą, nes kaip ir minėti tarptautiniai, ir Europos Sąjungos duomenų apsaugos teisės aktai, yra technologiškai neutralus. Asmens duomenų apsaugos įstatymo 1 straipsnio 3 dalyje yra nustatyta, kad minėtas įstatymas taikomas kartu su BDAR, kuris nacionalinėje teisės sistemoje yra taikomas tiesiogiai. Paminėtina, kad dirbtinį intelektą reguliuojančių ir įstatymo galią turinčių nacionalinių teisės aktų nėra.

Antrinių duomenų apsaugos teisės šaltinių yra gausu. Svarbiausi *soft law* šaltiniai yra kompetentingų institucijų ir ekspertų priimtos, formaliai neprivalomos, tačiau autoritetingos nuomonės, rekomendacijos ar gairės (Zaleskis, 2019, p. 63). Bene viena iš svarbiausių tarptautinių *soft law* šaltinių yra Ekonominio bendradarbiavimo ir plėtros organizacijos gairės dėl privatumo apsaugos ir tarptautinių asmens duomenų srautų (Ekonominio bendradarbiavimo ir plėtros organizacijos gairės dėl privatumo apsaugos ir tarptautinių..., 1980) (toliau – **EBPO privatumo gairės**), kuriose įtvirtinti pagrindiniai duomenų apsaugos teisės principai (Zaleskis, 2019, p. 66). Taip pat, duomenų apsaugos teisei yra aktualios 29 straipsnio duomenų apsaugos darbo grupės ir Europos duomenų apsaugos valdybos nuomonės ir gairės bei Europos Sąjungos duomenų apsaugos priežiūros pareigūno nuomonės. Minėtų *soft law* nuomonių ar gairių dėl dirbtinio intelekto įtakos asmens duomenų apsaugai vis dar nėra. Tačiau šiame darbe bus nagrinėjamos minėtų institucijų ir pareigūno nuomonės ir gairės, siekiant analizuoti BDAR nuostatas, kurios nulemia BDAR principų taikymo sritį. Paminėtinos 29 straipsnio duomenų apsaugos darbo grupės nuomonės ir gairės, kurios yra svarbios nagrinėjant BDAR taikymą: gairės dėl automatizuoto atskirų sprendimų priėmimo ir profiliavimo, skaidrumo užtikrinimo gairės, nuomonė dėl asmens duomenų sąvokos. Atkreiptinas dėmesys, kad priėmus BDAR, 29 straipsnio duomenų apsaugos darbo grupę pakeitė Europos duomenų apsaugos valdyba. Minėta institucija *soft law* šaltiniais aiškina BDAR įtvirtintą teisinį reguliavimą.

Pavyzdžiui, aktualios gairės dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ ar dėl BDAR teritorinės taikymo srities.

Dirbtinio intelekto reguliavimo sritis Europos Sąjungos lygiu yra reglamentuota. Dar 2017 m. rugsėjo mėn. vykusiame Talino aukščiausiojo lygio susitikime skaitmeniniais klausimais Europos Vadovų Tarybos nurodė Europos Sąjungos Komisijai iki 2018 m. pateikti Europos požiūrį į dirbtinį intelektą ir paragino skubiai spręsti naujų technologijų tendencijų klausimą siekiant sėkmingai kurti skaitmeninę Europą (Europos Vadovų Tarybos susitiko išvada, 2017). Europos Sąjungos Komisija reaguodama į Europos Vadovų Tarybos raginimus, priėmė komunikatą „Dirbtinis intelektas Europai“, kuriuo yra įtvirtinama pirmoji Europos Sąjungos dirbtinio intelekto strategija (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018). Komunikatu nustatoma vizija, kuria siekiama užtikrinti, kad Europos Sąjunga atliktų pagrindinį vaidmenį pasaulyje plėtojant dirbtinio intelekto politiką, sprendžiant su dirbtiniu intelektu susijusius klausimus ir visapusiškai išnaudojant ekonominę dirbtinio intelekto diegimo naudą (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018). 2018 m. Europos Sąjungos Komisija priėmė Suderintą dirbtinio intelekto planą, kuriame išdėstė veiksmus dėl dirbtinio intelekto plėtros. Europos Komisija ragina didinti investicijas į dirbtinį intelektą, stiprinti dirbtinio intelekto mokslinius tyrimus ir remti etišką dirbtinio intelekto plėtrą. Minėtame akte valstybės narės buvo raginamos parengti nacionalines dirbtinio intelekto strategijas (Europos Komisijos Komunikatas Suderintas dirbtinio intelekto planas, 2018). Lietuvos Respublika, įgyvendindama Europos Sąjungos Komisijos raginimus, priėmė „Lietuvos dirbtinio intelekto strategiją“, išreikšdama tikslą tapti dirbtinio intelekto lydere regione (Lietuvos dirbtinio intelekto strategija. Ateities..., 2022). 2021 m. Europos Sąjungos Komisija žengė svarbų žingsnį, kuriuo pasiūlė Dirbtinio intelekto aktą. Dirbtinio intelekto aktu siekiama teisėto, saugaus ir patikimo dirbtinio intelekto naudojimo. Nors dirbtinio intelekto aktas vis dar yra nepriimtas, tačiau susilaukė kritikos dėl teisinio aiškumo trūkumų. Dirbtinio intelekto akto aiškinamajame memorandume yra nurodyta, kad jis nedaro poveikio BDAR. Tačiau Dirbtinio intelekto akte mažai aiškumo dėl duomenų tvarkymo bet kokiomis kitomis dirbtinio intelekto sistemomis, išskyrus didelės rizikos dirbtino intelekto sistemas. Tačiau net ir didelės rizikos dirbtinio intelekto sistemų atveju daugiausia dėmesio skiriama specialių kategorijų asmens duomenis. Pavyzdžiui, Dirbtinio intelekto akto 10 straipsnyje reglamentuojamas duomenų rinkimas, patvirtinimas ir testavimas, tačiau nepateikiama nuorodų į asmens duomenų subjektų teises.

Taigi, duomenų apsaugos teisei yra taikomi tiek tarptautiniai, Europos Sąjungos, nacionaliniai, tiek pirminiai ir antriniai teisės šaltiniai. Dirbtinį intelektą Europos Sąjungos

lygiu yra siekiama sureguliuoti. Šiam tikslui pateiktas pasiūlymas dėl Dirbtinio intelekto akto. Atitinkamai, šis darbas bus pagrįstas duomenų apsaugos teisės šaltiniais ir naujausiais Europos Sąjungos teisės aktais, kuriais siekiama reguliuoti dirbtinį intelektą.

2. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TAIKYMO DIRBTINIAM INTELEKTUI APIMTIS

2.1. Asmens duomenų sąvoka

Duomenų apsaugos materialinę taikymo sritį lemia asmens duomenų samprata (Zaleskis, 2019, p. 91). Tai reiškia, kad asmens duomenų sąvoka yra ribinė taikant duomenų apsaugos teisę (Kuner *et al.*, 2020, p. 105). Todėl kiekvieną kartą, siekiant nustatyti, ar BDAR nuostatos yra taikomos, reikia išsiaiškinti, kokia informacija sudaro asmens duomenis. Šioje dalyje bus pateikiama asmens duomenų sampratos analizė ir jų sąsaja su dirbtiniu intelektu.

BDAR 4 straipsnio 1 punkte nustatyta, kad asmens duomenys yra „bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti“. Specialiojoje literatūroje ir *soft law* šaltiniuose nurodoma, kad minėtą normą sudaro keturi pagrindiniai elementai (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 5): (1) „bet kokia informacija“; (2) „informacija, susijusi su asmeniu“; (3) „asmuo, kurio tapatybė gali būti nustatyta“; (4) fizinis asmuo (Marengo, 2021, p. 33). Išvardintų elementų analizė atskleidžia sąvokos „asmens duomenys“ sampratą. Atitinkamai, kiekvienas asmens duomenų sąvokos elementas bus nagrinėjamas plačiau, siekiant atskleisti sąsajas tarp asmens duomenų sampratos ir dirbtinio intelekto.

Pirmasis elementas „bet kokia informacija“ atspindi Europos Sąjungos įstatymų leidėjo valią asmens duomenų sąvokai suteikti plačią reikšmę, kuri neapsiribotų neskelbtina ar asmeninio pobūdžio informacija, o apimtų bet kokią informaciją, t. y. tiek objektyvią (pvz., informaciją apie atitinkamos medžiagos būvimą kraujyje), tiek subjektyvią (pvz., nuomonę ar vertinimą) (Europos Sąjungos Teisingumo Teismo 2017 m. gruodžio 20 d. sprendimas *Nowak* byloje), neatsižvelgiant į informacijos formatą ar techninę laikmeną, kurioje ji pateikiama. Todėl informacija gali būti pateikiama rašytine forma, skaičiais, fotografiniu vaizdu ar garsu (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 7-8). Tiek Europos Sąjungos, tiek nacionalinėje teismų praktikoje yra aiškinama, kas sudaro asmens duomenų elementą „bet kokia informacija“: telefono numeris, informacija, susijusi su asmens darbo sąlygomis ar pomėgiais (Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 6 d. sprendimas *Lindqvist*); automobilio valstybinis numeris, automobilio modelis, automobilio pagaminimo metai (Lietuvos vyriausio administracinio teismo 2012 m. liepos 26 d. nutartis administracinėje byloje); duomenys apie asmens pajamas ir mokesčius (Europos Sąjungos Teisingumo Teismo 2003 m. gegužės 20 d. sprendimas *Lauermann*); egzaminuotojo rašytiniai atsakymai (Europos Sąjungos Teisingumo Teismo

2017 m. gruodžio 20 d. sprendimas *Nowak*); informacija apie asmeniui priklausantį turtą (Vilniaus apygardos administracinio teismo 2020 m. gegužės 28 d. sprendimas administracinėje byloje); pirštų atspaudai (Europos Sąjungos Teisingumo Teismo 2013 m. spalio 17 d. sprendimas *Schwarz*); vaizdo įraše užfiksuotas asmens atvaizdas (Europos Sąjungos Teisingumo Teismo 2014 m. gruodžio 11 d. sprendimas *Ryneš*); judriojo ryšio įrangos naudojo būtinieji duomenys, be kita ko, naudotojo vardas, pavardė, pavadinimas, adresas, telefono numeriai, į kuriuos ir iš kurių skambinta (Europos Sąjungos Teisingumo Teismo 2014 m. balandžio 8 d. sprendimas *Digital Rights Ireland ir Seitlinger ir kt.*); dinaminis IP adresas (Europos Sąjungos Teisingumo Teismo 2016 m. spalio 19 d. sprendimas *Breyer*). Dirbtinio intelekto kontekste informacija nėra atribojama, todėl į duomenų apsaugą patenka daug įvairių asmens duomenų. Dirbtinis intelektas didžiulius duomenų kiekius renka kiekvieną sekundę iš įvairių fizinių objektų teikiančių duomenis (pvz., jutiklių automobiliuose ir mobiliuosiuose telefonuose, pirštų atspaudų, veido bruožų ar biometrinio atpažinimo technologijų) ar stebėjimo prietaisų (pvz., eismo kamerų ar įeigos kontrolės sistemų). Taip pat, dirbtinis intelektas gali pasitelkti informaciją gautą iš tikslinės reklamos, kuri grindžiama įrašais, susijusiais su vartotojų savybėmis ir elgsena (pvz., lytimi, amžiumi, socialiniu gyvenimu, pirkimo ir naršymo internete istorija). Dirbtinis intelektas gali vertinti paraiškas dėl darbo, remdamasis įrašais, kuriuose darbuotojų charakteristikos (pvz., išsilavinimas, įsidarbinimo istorija, protinių gebėjimų testų rezultatai) susiejamos su jų darbo rezultatais. Prognozuojant konkretaus nusikaltėlio pakartotinio nusikaltimo tikimybę, dirbtinis intelektas gali remtis įrašais, kuriuose susiejamos ankstesnių nusikalstamą veiką padariusių asmenų charakteristikos (pvz., jų išsilavinimas, įsidarbinimo istorija, šeiminė padėtis, teistumas, psichologinių testų rezultatai). Siekiant pasiūlyti individualų gydymą, dirbtinio intelekto siūlymas gali būti grindžiamas ankstesnių pacientų įrašais, kuriuose jų charakteristikos ir medicininiai tyrimai susiejami su vėlesnėmis sveikatos būklėmis, ir gydymu. Atitinkamai, tai suponuoja, kad dirbtinis intelektas gali rinkti įvairią informaciją iš įvairių šaltinių, kuri gali apimti itin platų informacijos spektrą (t. y. duomenis apie asmens lytį, amžių, išsilavinimą ar net medicininius įrašus).

Antrasis elementas „informacija, susijusiu su asmeniu“ reiškia, kad informacija turi būti apie asmenį (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 9). Informacija susijusiu su asmeniu gali būti tiesiogiai arba netiesiogiai (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 9). Europos Sąjungos Teisingumo Teismo praktika aiškinant minėtą antrąjį asmens duomenų sąvokos elementą nėra nuosekli (Marengo, 2021, p. 34). Pavyzdžiui, 2014 m. byloje dėl galimybės susipažinti su prieglobsčio prašytojo bylos

duomenimis, Europos Sąjungos Teisingumo Teismas „informacija, susijusią su asmeniu“ vertino siaurai. Nors laikėsi pozicijos, kad prieglobsčio prašytojo asmenvardis, gimimo data, pilietybė, lytis, religija ar kalba, yra informacija, susijusi su fiziniu asmeniu, todėl šiuos duomenis reikia laikyti asmens duomenimis, tačiau konstatavo, kad prieglobsčio byloje parengiamuosiuose dokumentuose esanti teisinė analizė, nors ir gali būti susijusiu su fiziniu asmeniu, nėra asmens duomenys (Europos Sąjungos Teisingumo Teismo 2014 m. liepos 17 d. sprendimas *YS ir kt.* byloje C-141/12). Visgi, vėlesnėje, 2017 m. praktikoje, Europos Sąjungos Teisingumo Teismas laikėsi ekspansyvios pozicijos (Europos Sąjungos Teisingumo Teismo 2017 m. gruodžio 20 d. sprendimas *Nowak*). Europos Sąjungos Teisingumo Teismas nusprendė, kad egzaminuotojo pateiktos rašytinės pastabos yra asmens duomenys, nes informacija yra „susijusi“ su fiziniu asmeniu, atsižvelgiant į informacijos turinį, tikslą ir poveikį konkrečiam asmeniui (Europos Sąjungos Teisingumo Teismo 2017 m. gruodžio 20 d. sprendimas *Nowak*). Nepaisant praktikos nepastovumo, darytina išvada, kad naujausia teismo praktika laikosi plačios pozicijos aiškindama asmens duomenų sampratos elementą „informacija, susijusi su asmeniu“ (Kuner *et al.*, 2020, p. 110). Dirbtinio intelekto kontekste, surinkta informacija taip pat turėtų būti aiškinama plačiai. Ne kartą buvo minėta, kad dirbtinis intelektas yra pagrįstas didelių duomenų kiekių rinkimu, todėl naudojant dirbtinį intelektą, informacija gali būti susiejama su asmeniu tiek tiesiogiai (pvz., dirbtiniam intelektui apdorojant paciento medicininių tyrimų rezultatus), tiek netiesiogiai (pvz., naudojant dirbtinio intelekto pagrįstą programą, kuri galėtų identifikuoti asmenį pagal parduodamo namo vertę).

Trečiasis elementas „asmuo, kuriuo tapatybė gali būti nustatyta“ turėtų būti aiškinamas lanksčiai, nes fizinio asmens tapatybę yra galima nustatyti, jei atitinkamas asmuo yra išskiriamas iš kitų asmenų (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 12). Asmens tapatybė yra nustatoma tiesiogiai, t. y. pagal informaciją, kuri yra glaudžiai susijusiu su konkrečiu asmeniu (pvz., pagal vardą ir pavardę, plaukų spalvą, profesiją ar pareigas) (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 12) ir netiesiogiai, t. y. pagal informaciją, kuri savaime neleidžia nustatyti atitinkamo asmens tapatybės (pvz., pagal dinaminį IP adresą) (Europos Sąjungos Teisingumo Teismo 2016 m. spalio 19 d. sprendimas *Breyer*). Be to, norint įvertinti, ar asmens tapatybė gali būti nustatyta, reikia atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo duomenų subjekto tapatybei nustatyti (BDAR 26 konstatuojamoji dalis). Tai reiškia, kad šis kriterijus yra tenkinamas, kai fizinio asmens tapatybę yra įmanoma nustatyti, nesiimant neproporcingai didelių pastangų laiko, išlaidų ir žmogiškųjų išteklių požiūriu (Kuner *et al.*, 2020, p. 111). Dirbtinio intelekto kontekste tai reiškia, kad visas

dirbtinio intelekto projektavimas, kūrimas ar naudojimas yra atliekamos iš įvairių rūšių asmens duomenų tvarkymo operacijų, kurių pagalba asmens tapatybė gali būti nustatyta. Minėta, kad apdorojant dirbtinį intelektą naudojami dideli duomenų kiekiai. Dirbtinis intelektas renka asmens duomenis plačiu mastu (pvz., iš mobiliųjų telefonų, automobilių ar kitų prietaisų jutiklių) ir vis pažangiau dirba su surinktais duomenimis (pvz., naudoja veido bruožų, pirštų atspaudų ar net biometrinio atpažinimo technologijas). Atitinkamai, ši plati asmens duomenų rinkimo diskrecija gali suteikti dirbtiniam intelektui galimybių asmens duomenis sujungti taip, kad būtų galima identifikuoti asmens tapatybę tiek tiesiogiai, tiek netiesiogiai.

Ketvirtasis elementas „fizinis asmuo“ reiškia, kad asmens duomenų apsauga yra užtikrinama žmonėms. Valstybių narių nacionaliniuose aktuose tiksliau apibrėžiama žmogaus sąvoka (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 21). Pavyzdžiui, Lietuvos Respublikos civilinio kodekso 2.2 straipsnio 1 dalyje nustatoma, kad fizinio asmens civilinis teisnumas atsiranda asmens gimimo momentu ir išnyksta, jam mirus (Lietuvos Respublikos civilinis kodeksas, 2020). Atitinkamai, tai reiškia, kad asmens duomenų apsauga yra užtikrinama gyviems asmenims, o BDAR 4 straipsnio 1 dalis neapima asmens duomenų apie mirusius asmenis. Be to, pagal bendrąją taisyklę, juridinių asmens duomenys BDAR nėra saugomi (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 22). Tačiau Europos Sąjungos Teisingumo Teismo praktikoje yra išaiškinta, kad juridiniai asmenys gali reikalauti duomenų apsaugos remiantis Europos Sąjungos pagrindinių teisių chartijos 8 straipsniu tuo atveju, jei pagal oficialų juridinio asmens pavadinimą yra galima nustatyti vieną ar daugiau fizinių asmenų (Europos Sąjungos Teisingumo Teismo 2010 m. lapkričio 9 d. sprendimas *Volker und Markus Schecke ir Eifert*). Dirbtinio intelekto kontekste, minėta, kad dirbtiniam intelektui generuojant itin didelius informacijos kiekius, dalis šios informacija būna susijusi su fiziniu asmeniu. Pavyzdžiui, jau keletą metų plačiai paplitusi Lietuvoje Jungtinių Amerikos Valstijų filmų transliacijų kompanija, teikianti pasaulines vaizdo formato transliavimo paslaugas internetu „Netflix“, kurią kiekvieną dieną pasaulyje naudoja daugiau 220 mln. (Netflix Recommendations: How Netflix Uses, 2023) žmonių, naudoja dirbtinį intelektą, kuris renka informaciją apie asmens žiūrėjimo įpročius ir pagal šiuos duomenis pateikia rekomendacijas. Todėl akivaizdu, kad tokios informacijos rinkimas visais atvejais bus susijęs su fiziniu asmeniu. Be to, kaip buvo minėta, dirbtinis intelektas generuoja didelį kiekį informacijos, į kurią patenka įvairių asmens duomenų, todėl neabejotina, kad informacija gali būti susijusi ir su juridiniais asmenimis. Atitinkamai, tai suponuoja, kad

dirbtinio intelekto naudojimas yra neatsiejamas nuo informacijos apie fizinį asmenį ar net juridinį asmenį.

Taigi, vertinant, ar dirbtinio intelekto generuojami duomenys yra asmens duomenys, reikia atsižvelgti į BDAR materialinę taikymo sritį. Europos Sąjungos duomenų apsaugos teisėje, asmens duomenų samprata aiškinama plačiai, todėl darytina išvada, kad dirbtinio intelekto renkama informacija apims asmens duomenis.

2.2. Duomenų valdytojo ir tvarkytojo vaidmuo dirbtiniame intelekte

Sąvokos „duomenų valdytojas“ ir „duomenų tvarkytojas“ yra esminės taikant BDAR. Šių sąvokų identifikavimas reikšmingas siekiant nustatyti, kas yra atsakingas už BDAR nuostatų laikymąsi (Europos duomenų apsaugos valdyba, 2021, p. 3). Atitinkamai, šioje dalyje bus analizuojamos duomenų valdytojo ir duomenų tvarkytojo sąvokos ir jų funkcijų santykis su dirbtiniu intelektu.

BDAR 4 straipsnio 7 dalyje nustatyta, kad „duomenų valdytojas yra fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones <...>“. Konkrečiai, duomenų valdytojo sąvoka turėtų būti aiškinama plačiai kaip apimanti tiek organizacijas, privačius asmenis, asmenų grupes (Europos duomenų apsaugos valdyba, 2010a, p. 12), tiek viešuosius asmenis (pvz., parlamento komitetą) (Europos Sąjungos Teisingumo Teismo 2020 m. liepos 9 d. spendimas *Land Hessen*). Specialiojoje literatūroje pripažįstama, kad pagrindinė duomenų valdytojo savybė yra savarankiškumas nustatant duomenų tvarkymo tikslus ir priemones (Zaleskis, 2019, p. 100). Tai reiškia, kad duomenų valdytojas turi turėti galimybę daryti įtaką nustant fizinio asmens duomenų tvarkymo tikslus (t. y. kodėl asmens duomenys tvarkomi) ir priemones (t. y. kaip asmens duomenys tvarkomi) (Europos duomenų apsaugos valdyba, 2021, p. 3), bet nebūtinai pats turi atlikti faktinį duomenų tvarkymą (Zaleskis, 2019, p. 99). Kiekvienu atveju, siekiant nustatyti, kas iniciavo duomenų tvarkymo tikslus ir priemones, reikia vertinti konkrečias duomenų tvarkymo operacijas ir suprasti, kas jas nustatė (Zaleskis, 2019, p. 100). Be to, duomenų valdytojo samprata yra neatsiejama nuo duomenų valdytojo atsakomybės, kuri yra vertinama ne formaliai, o atsižvelgiant į faktinę duomenų valdymo įtaką (Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*). Duomenų valdytojas yra atsakingas, kad būtų laikomasi su asmens duomenų tvarkymu susijusių principų ir turi sugebėti įrodyti, kad jų laikosi (BDAR 5 straipsnio 2 dalis). BDAR nuostatos į dirbtinį intelektą, kaip duomenų valdytoją, nereferuoja (Europos Sąjungos pagrindinių teisių

agentūra *et al.,* 2018, p. 368). Tačiau dirbtinio intelekto naudojimas tvarkant asmens duomenis yra sudėtingas, ypač dirbtinio intelekto atsakomybės kontekste, dėl to, kad dirbtinis intelektas gali priimti sprendimą, pagrįstą jo paties plėtojamu duomenų tvarkymu. Vis dėlto, Europos Sąjungos institucijos laikosi požiūrio, kad dirbtinio intelekto atliekamus procesus privalo koordinuoti žmogus, jei dirbtinis intelektas yra pagrįstas asmens duomenų tvarkymu arba tvarko asmens duomenis užduočiai atlikti (Europos ekonomikos ir socialinių reikalų komiteto nuomonė „Skaitmeninė tapatybė, duomenų suverenumas ir..., 2022). Tai suponuoja išvadą, kad asmens duomenų teises kylančias iš BDAR privalo užtikrinti duomenų valdytojas, t. y. subjektas, kuris priima sprendimus dėl dirbtinio intelekto tikslų ir priemonių. Atkreiptinas dėmesys į tai, kad jei paslaugos tiekėjas suteikia dirbtinio intelekto įrankius klientams (pvz., juridiniams asmenims) ir nenaudoja asmens duomenų savo tikslams, šis subjektas yra duomenų tvarkytojas, o klientas – duomenų valdytojas. Vis dėlto, praktiniu požiūriu gali kilti neaiškumų, nes duomenų valdytojai ne visada gali būti subjektai, turintys faktinę, ekonominę ar praktinę galią duomenų tvarkymo operacijoms. Neretai duomenų valdytojams gali būti sudėtinga užtikrinti, kad jų naudojama dirbtinio intelekto sistema atitinka BDAR reikalavimus, kuri dažniausiai yra pasaulinių tiekėjų produktas.

Asmenys, kurie tvarko asmens duomenis duomenų valdytojo vardu ir tik pagal jo nurodymus, laikytini duomenų tvarkytojais (Kuner *et al.*, 2020, p. 159). Duomenų tvarkytojas apibrėžiamas kaip „fizinis ar juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri kaip buvo minėta, duomenų valdytojo vardu tvarko asmens duomenis“ (BDAR 4 straipsnis 8 punktas). Tai reiškia, kad duomenų tvarkytojas apibrėžiamas pagal dvi sąlygas: (1) jis turi būti „atskiras subjektas“ ir (2) turi „tvarkyti asmens duomenis duomenų valdytojo vardu“ (Marengo, 2021, p. 41). Pirmas elementas „atskiras subjektas“ reiškia duomenų valdytojo pasirinkimą duomenų tvarkymą perduoti kitam subjektui (Europos duomenų apsaugos valdyba, 2021, p. 26). Antrasis elementas „tvarkyti asmens duomenis duomenų valdytojo vardu“ reiškia, kad duomenų tvarkytojas įgyvendina duomenų valdytojo nurodymus dėl duomenų tvarkymo tikslų ir priemonių (Europos Sąjungos Teisingumo Teismo 2019 m. liepos 29 d. sprendimas *Fashion ID* cituota Kuner *et al.,* 2020, p. 159) ir veikia tiesiogiai nekontroliuojant duomenų valdytojui (Europos duomenų apsaugos valdyba, 2021, p. 27). Tai suponuoja, kad duomenų tvarkytojo buvimas priklauso nuo duomenų valdytojo sprendimo ir pagrindinis duomenų tvarkytojo skirtumas nuo duomenų valdytojo yra nesavarankiškumas tvarkant asmens duomenis (Zaleskis, 2019, p. 101-102). Minėta, kad atsakomybė dėl dirbtinio intelekto naudojimo ir jo atitikties BDAR tenka duomenų valdytojui, o duomenų tvarkytojo pareigos yra ribotos. Duomenų

tvarkytojas yra atsakingas ribota apimtimi ir atsakomybė kyla tik konkrečiais BDAR nustatytais atvejais (pvz., duomenų tvarkytojas turi pareigą tvarkyti duomenis tik pagal duomenų valdytojo pateiktus nurodymus (Zaleskis, 2019, p. 102). Vis dėlto, kai kurios dirbtiniu intelektu pagrįstos paslaugos (pvz., asmens duomenų saugojimas debesijoje) gali patekti į duomenų tvarkytojo apibrėžti (Europos duomenų apsaugos valdyba, 2021, p. 14), tačiau programinės ar techninės įrangos pardavėjams BDAR tiesiogiai netaikomas. Tai suponuoja, kad duomenų valdytojai privalo pasinaudoti techninėmis ir organizacinėmis priemonėmis, kad užtikrintų, jog minėti subjektai teiktų BDAR atitinkančius produktus.

Duomenų tvarkytojo ir duomenų valdytojo sąvokos yra susijusios. Kaip buvo minėta, duomenų tvarkytojas yra neatsiejamas nuo duomenų valdytojo, kurio vardu tvarko asmens duomenis (BDAR 4 straipsnis 8 dalis), užtikrindamas duomenų valdytojo apibrėžtus asmens duomenų tvarkymo tikslus ir priemones (BDAR 4 straipsnis 7 dalis). Tuo tarpu, duomenų valdytojas turi pareigą pasitelkti tik tuos duomenų tvarkytojus, kurie tvarkydami asmens duomenis užtikrina tinkamas technines ir organizacines priemones (pvz., tinkamą asmens duomenų saugumą ar ekspertines žinias apie asmens duomenų pažeidimus) (Europos duomenų apsaugos valdyba, 2021, p. 31-32). Tačiau kai asmens duomenys tvarkomi pasitelkiant dirbtinį intelektą, gali būti sudėtinga atskirti duomenų valdytoją ir duomenų tvarkytoją. Kaip buvo minėta, dirbtinis intelektas yra pagrįsta dideliais duomenų kiekiais, sąsajų ieškojimu, prognozių ir sprendimų priėmimu, todėl gali kilti neaiškumų, vertinant, kas konkrečiai nustatė duomenų tvarkymo tikslus ir priemones. Tokia situacija galėtų susidaryti, jei įmonė perduotų duomenų analizę kitai bendrovei, kuri specializuojasi dirbtinio intelekto srityje. Specialiojoje literatūroje rekomenduojama tokiais atvejais duomenų valdytojui ir duomenų tvarkytojui sudaryti sutartį, kurioje būtų aiškiai nurodyta, kaip asmens duomenys turi būti tvarkomi (Information Commissioner's Office, 2017, p. 57). Vis dėlto, sutarties sudarymas nėra sprendimo būdas, jei duomenų tvarkytojas turėtų pakankamai laisvės priimti sprendimus, kokie duomenys turi būti renkami ir kaip turėtų būti taikomi analizės metodai.

Kaip buvo aptarta anksčiau, pagrindiniai subjektai, kurie turi įgyvendinti BDAR reikalavimus yra duomenų valdytojas ir duomenų tvarkytojas. Dirbtinio intelekto akte atsakomybė dėl dirbtinio intelekto naudojimo daugiausia dėmesio skiriama subjektams, kurie kuria, parduoda arba naudoja dirbtinį intelektą komerciniais tikslais, t. y. tiekėjams ir naudotojams (Dirbtinio intelekto aktas 3 skyrius), tačiau nėra detalizuojama, kokia apimtimi šie subjektai privalo užtikrinti asmens duomenų apsaugą. Galėtų susidaryti situaciją, kai naudotojai pagal Dirbtinio intelekto aktą galėtų būti kvalifikuojami kaip duomenų valdytojai pagal BDAR. Pagal Dirbtinio intelekto akto 29 straipsnį, naudotojai

turi ribotas pareigas. Tačiau kaip dirbtinio intelekto naudotojas, jis gali naudoti ir asmens duomenis. Atitinkamai, gali kilti klausimas dėl pareigų kylančių pagal BDAR. Tuo tarpu, tikėtina, kad tiekėjai galėtų būti kvalifikuojami kaip duomenų tvarkytojai, ypač jei jie teikia dirbtinio intelekto sistemų priežiūros paslaugas, susijusias su asmens duomenų tvarkymu naudotoju vardu ir pagal jo nurodymus (Vale, 2022). Taigi, toks tiekėjo ir naudojo apibrėžimas pagal Dirbtinio intelekto aktą gali sukelti neaiškumo BDAR kontekste. Todėl siekiant užtikrinti tinkamą pareigų vykdymą, kai naudojamas dirbtinis intelektas, kuris tvarko asmens duomenis, reikalinga veiksminga sąveika tarp BDAR ir Dirbtinio intelekto akto (Jelinek, 2022).

Taigi, duomenų valdytojo ir tvarkytojo prasme, kai asmens duomenys yra tvarkomi naudojant dirbtinį intelektą, duomenų valdytoju pripažįstamas subjektas, kuris priima sprendimus dėl dirbtinio intelekto tikslų ir priemonių, o duomenų tvarkytojas yra asmuo, kuris tvarko asmens duomenis duomenų valdytojo vardu ir nenaudoja asmens duomenų savo tikslams.

2.3. Duomenų subjektas

Sąvoką „duomenų subjektas“ yra glaudžiai susijusi su asmens duomenų samprata. Tai reiškia, kad surinkti asmens duomenys kiekvienu atveju bus konkrečiai susiję su duomenų subjektu. Siekiant užtikrinti tinkamą asmens duomenų apsaugą, būtina identifikuoti asmens duomenų subjektą. Atitinkamai, šioje dalyje bus aptariama duomenų subjekto sąvoka ir apibrėžiamas dirbtinio intelekto tvarkomų asmens duomenų subjektas.

BDAR 4 straipsnio 1 dalis nustato, kad duomenų subjektas yra fizinis asmuo, kurio tapatybę tiesiogiai ar netiesiogiai yra galima nustatyti. Tai reiškia, kad fizinio asmens tapatybę galima nustatyti tiesiogiai (pvz., pagal vardą ir pavardę, el. paštą) ir netiesiogiai (29 straipsnio duomenų apsaugos darbo grupė, 2007, p. 12-13) (pvz., pagal internetinį identifikatorių). Dirbtinio intelekto kontekste, duomenų subjektu dažniausiai galima laikyti fizinius asmenis, apie kuriuos dirbtinis intelektas renka informaciją. Informaciją apie fizinį asmenį gali būti renkama iš įvairių šaltinių, pavyzdžiui, jutiklių automobiliuose ir mobiliuosiuose telefonuose, naudojamų programėlių (pvz., Facebook „like“ paspaudimų), pirštų atspaudų ar veido bruožų.

Atitinkami, galima daryti išvadą, kad fizinis asmuo, kurio duomenys yra tvarkomi dirbtinio intelekto, yra laikomas duomenų subjektu pagal duomenų apsaugos teisę, kuri užtikrina jo teises pagal BDAR.

2.4. Teritorinė Bendrojo duomenų apsaugos reglamento taikymo sritis

BDAR teritoriniu taikymu yra išplečiama Europos Sąjungos asmens duomenų apsaugos teisės sritis, siekiant užtikrinti vienodas sąlygas tiek Europos Sąjungos, tiek už Europos Sąjungos ribų veikiantiems subjektams, kurie vykdo veiklą Europos Sąjungos rinkoje (Albrecht, 2016, p. 476). Teritorinio taikymo sritis yra viena iš svarbiausių BDAR nuostatų, nes jei duomenų tvarkymas nepatenka į teritorinio taikymo sritį, BDAR yra netaikomas (Kuner *et al.*, 2020, p. 82). Todėl šioje dalyje bus nagrinėjama BDAR 3 straipsnyje reglamentuojama BDAR teritorinio taikymo sritis ir jos sankirta su dirbtiniu intelektu.

BDAR 3 straipsnio 1 dalyje nustatomas BDAR taikymas asmens duomenų tvarkymui, kai tokią veiklą vykdo duomenų valdytojo ar duomenų tvarkymo buveinė, vykdydama savo veiklą, nepaisant faktinės duomenų tvarkymo vietos. Tai reiškia, kad visų pirma, duomenų valdytojas ar duomenų tvarkytojas turi būti įsisteigęs Europos Sąjungoje buveinę (Europos duomenų apsaugos valdyba, 2019, p. 5), kuri per stabilią struktūrą, vykdo veiksmingą ir realią veiklą (BDAR 22 konstatuojamoji dalis) (pvz., filialą ar dukterinę bendrovę) (Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*). Antra, asmens duomenys turi būti tvarkomi „įmonės veiklos kontekste“, kai įmonės veikla yra neatskiriamai susijusi su jos įsteigimo veikla (Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*). Atitinkamai, duomenų valdytojui arba duomenų tvarkytojui reikės laikytis BDAR nustatyto reglamentavimo, jeigu Europos Sąjungoje turi savo buveinę, kuri vykdo veiklą. Dirbtiniam intelektui BDAR taikomas, kai dirbtinį intelektą naudoja įmonės, kurios turi buveinę Europos Sąjungoje. Pavyzdžiui, Jungtinių Amerikos Valstijų informacinių technologijų bendrovė „Apple“, kuri naudoja kalbos atpažinimo programą „Siri“ yra įsteigusi filialus Austrijoje, Belgijoje, Danijoje, Suomijoje ir kitose Europos Sąjungos valstybėse narėse. Atitinkamai, minėta įmonė yra įsteigusi Europos Sąjungoje, todėl yra įpareigota, kaip duomenų valdytoja, tvarkyti asmens duomenis pagal BDAR.

BDAR 3 straipsnio 2 dalyje nustatomas eksteritorialus BDAR taikymas duomenų valdytojas ir duomenų tvarkytojams, neįsisteigusiam Europos Sąjungoje. Siekiant taikyti minėtą BDAR normą, reikia nustatyti (1) ar duomenys yra susiję su duomenų subjektu; (2) ar duomenų tvarkymas yra susijęs su prekių ar paslaugų siūlymų, arba duomenų subjektų elgesio stebėsena Europos Sąjungoje (Europos duomenų apsaugos valdyba, 2019, p. 14). Pirmąjį kriterijų reikia aiškinti plačiai, neatsižvelgiant į duomenų subjekto pilietybę ar teisinį statusą (Kuner *et al.*, 2020, p. 88). Antrasis kriterijus turėtų būti tikslingai nukreiptas į duomenų subjektą, t. y. į prekių ir paslaugų siūlymą arba elgesio stebėseną,

neatsižvelgiant į pasiūlymo ar vykdymo stebėjimo trukmę (Europos duomenų apsaugos valdyba, 2019, p. 15). Pavyzdžiui, tarptautinių technologijų bendrovė „Meta Platforms, Inc.“, įsisteigusi Jungtinėse Amerikos Valstijose naudoja dirbtinį intelektą produktuose „Facebook“ ar „Instagram“, Europos Sąjungos duomenų subjektams pateikdama pasiūlymus arba prekes pagal konkretaus fizinio asmens surinktus duomenis. Taip pat, BDAR gali būti taikomas, kai duomenų tvarkymas yra susijęs su duomenų subjektų elgesio stebėsena Europos Sąjungoje. Pavyzdžiui, Jungtinių Amerikos Valstijų įmonė „Google Nest“ siūlo Europos Sąjungos valstybių narių vartotojams išmaniuosius įrenginius, kurie geba rinkti asmens duomenis ir stebėti vartotojų elgseną (pvz., išmaniuosius namų asistentus). Atitinkamai, dėl minėtų technologijų, kurios yra pagrįstos dirbtiniu intelektu, jų atliekamas duomenų tvarkymas patenka į BDAR taikymo sritį.

Kalbant apie teritorinio taikymo sritį, paminėtas ir Dirbtinio intelekto aktas. Priešingai nei duomenų valdytojo ir tvarkytojo apibrėžties kontekste, Dirbtinio intelekto akto teritorinio taikymo sritis koreliuoja su BDAR reguliavimu. Dirbtinio intelekto akto 2 straipsnyje nustatoma, kad Dirbtinio intelekto aktas turi būti taikomas ne tik valstybės narės teritorijoje esantiems dirbtinio intelekto naudotojams, bet ir paslaugų tiekėjams, kurie pateikia dirbtinio intelekto sistemas į Europos Sąjungos rinką arba pradeda jas naudoti Europos Sąjungoje, neatsižvelgiant į tai, ar jie yra įsisteigę Europos Sąjungoje. Be to, į teritorinio taikymo sritį pateks ir trečiųjų šalių tiekėjai bei dirbtinio intelekto sistemų naudotojai, jei jų sukuriama produkcija bus naudojama Europos Sąjungoje. Tai reiškia, kad dirbtinio intelekto akto, kaip ir BDAR taikymo sritis, peržengia Europos Sąjungos ribas (Zannoni *et al.*, 2022).

Atsižvelgiant į tai, kas buvo išdėstyta, galima daryti išvadą, kad BDAR dirbtinio intelekto kontekste bus taikomas tik tuomet, kai duomenų valdytojas arba / ir duomenų tvarkytoja turi buveinę Europos Sąjungoje arba jei duomenų valdytojas ar / ir duomenų tvarkytojas nėra įsikūręs Europos Sąjungoje, tačiau jų vykdoma duomenų tvarkymo veikla yra susijusi su prekių ar paslaugų arba duomenų subjektų elgesio stebėsena Europos Sąjungoje.

3. DUOMENŲ APSAUGOS PRINCIPAI IR JŲ TAIKYMAS DIRBTINIAM INTELEKTUI

3.1. Teisėtumo, sąžiningumo ir skaidrumo principas

Europos Tarybos duomenų apsaugos konvencijos 4 straipsnio b dalis ir EBPO privatumo gairių 7 straipsnyje įtvirtinti bendrieji duomenų apsaugos teisėje taikomi teisės principai. BDAR 5 straipsnio 1 dalies a punkte nustatyta, kad asmens duomenys turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu. Tai reiškia, kad teisėtumą, sąžiningumą ir skaidrumą galima laikyti atskirais duomenų apsaugos teisės principais (Zaleskis, 2019, p. 113), todėl šioje dalyje teisėtumo, sąžiningumo ir skaidrumo principai bus analizuojami atskirai.

Teisėtumo principas reiškia, kad asmens duomenys turi būti tvarkomi laikantis visų teisės aktuose nustatytų reikalavimų (Kuner *et al.*, 2020, p. 314). Tai reiškia, kad teisėtumo principu siekiama užtikrinti, kad duomenų tvarkymas atitiktų visus duomenų apsaugos teisės šaltinius (Zaleskis, 2019, p. 114), t. y. tiek tarptautinius, Europos Sąjungos, tiek nacionalinius įstatymus ar poįstatyminius teisės aktus. Be to, teisėtumo principas įtvirtina duomenų valdytojo pareigą užtikrinti, kad duomenų tvarkymas atitiks duomenų apsaugos teisės šaltinių tikslus, dvasią ir sistemą (Zaleskis, 2019, p. 114). BDAR komentare nurodoma, kad asmens duomenų tvarkymas bus laikomas teisėtu tik tuomet, kai jis atitiks įstatymus, sieks teisėto tikslo, bus būtinas ir proporcingas siekiam tikslui pasiekti (Kuner *et al.*, 2020, p. 314). Atitinkami, duomenų apsaugos teisės prasme, teisėtumo principas yra neatsiejamas nuo teisėtų asmens duomenų tvarkymo pagrindų (BDAR 40 konstatuojamoji dalis). Tai suponuoja, kad asmens duomenų tvarkymas laikomas teisėtu, jei jis atitinka BDAR 6 straipsnį, pagal kurį duomenų tvarkymas turi būti grindžiamas bent vienu iš šešių teisėtų asmens duomenų tvarkymo pagrindų.

Dirbtinio intelekto kontekste, kad duomenų tvarkymas būtų teisėtas BDAR 5 straipsnio 1 dalies a punkto prasme, jis privalo atitikti bent vieną teisėtą duomenų tvarkymo pagrindą įtvirtintą BDAR 6 straipsnio 1 dalyje. Teisėti duomenų tvarkymo pagrindai yra duomenų subjekto sutikimas, sutartis su duomenų subjektu, teisinės prievolės vykdymas, siekis apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus, užduotis viešojo intereso labui arba viešosios valdžios funkcijos atlikimas ir teisėti duomenų valdytojo ar trečiosios šalies interesai (BDAR 6 straipsnio 1 dalies a–f punktai). Tačiau siekiant pasitelkti dirbtinį intelektą asmens duomenų tvarkymui, yra neaišku, kuriais teisėtais duomenų tvarkymo pagrindais, asmens duomenys turėtų būti tvarkomi. Specialiojoje literatūroje yra nuomonių, kad asmens duomenų tvarkymas BDAR 6 straipsnio 1 dalies c–e punktų (t. y. teisinės prievolės vykdymu, siekiu apsaugoti

gyvybinius duomenų subjekto ar kito fizinio asmens interesus, užduoties vykdymu viešojo intereso labui arba vykdant viešosios valdžios funkciją) pagrindais yra minimaliai tikėtini, kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą (Paal, 2022, p. 297). Tuo tarpu, priešingai nei minėtais teisėtais duomenų tvarkymo pagrindais, duomenų subjekto sutikimas, sutartis su duomenų subjektu ir teisėti duomenų valdytojo ar trečiosios šalies interesai yra itin aktualūs kuriant ir naudojant dirbtinį intelektą (Information Commissioner's Office, 2017, p. 29). Analizuojant sutikimą, kaip teisėtą duomenų tvarkymo pagrindą, *soft law* praktikoje yra nurodyta, kad sutikimas turi būti duotas laisva valia, turi būti konkretus, pagrįstas informacija ir nedviprasmiškas (Europos duomenų apsaugos valdyba, 2020a, p. 7). Europos Sąjungos Teisingumo Teismo praktikoje yra išaiškinta, kad sutikimas turi būti išreiškiamas aktyviais veiksmais, susijęs su atitinkamu duomenų tvarkymu ir negali būti kildinamas iš valios pareiškimo, kurio dalykas skiriasi (Europos Sąjungos Teisingumo Teismo 2020 m. lapkričio 11 d. sprendimas *Orange Romania*). Šie aspektai itin aktualus dirbtiniam intelektui, kadangi pagal atlikus empirinius tyrimus, yra dvejojama, ar duomenų subjekto sutikimas gali būti duodamas laisva valia ir konkrečiai, kai neretai duomenų subjektas nesupranta šiuolaikinių duomenų srautų sudėtingumo (Biega, 2021, p. 53). Be to, reikalavimas duoti informuotą sutikimą kelia sunkumų tais atvejais, kai duomenų valdytojas tiksliai nežino ir negali numatyti, kaip ir kokiais tikslais asmens duomenis tvarkys savaime besimokantis dirbtinis intelektas (Paal, 2022, p. 297). Atitinkamai, dirbtinio intelekto kontekste, manytina, kad sutikimu grindžiamas teisėtas duomenų tvarkymo pagrindas yra labiau fiktyvūs nei praktiškai įgyvendinamas. Sutartis su duomenų subjektu, kaip teisėtas duomenų tvarkymo pagrindas yra pagrįstas būtinumo sąlyga, kuri reiškia, kad būtina nustatyti sutarties sudarymo esmę ir pagrindinį tikslą, pagal kuriuos tikrinama, ar tvarkyti asmens duomenis yra būtina vykdant sutartį (29 straipsnio duomenų apsaugos darbo grupė, 2014, p. 18). Praktikoje sutartis kaip teisėtas duomenų tvarkymo pagrindas yra aktualus, kai asmuo perka internetu, o svetainė turi tvarkyti asmens vardą, pavardę, adresą ir kredito kortelės duomenis, kad užsakymas būtų įvykdytas. Tačiau dirbtiniu intelektu pagrįsta analizė, pagal savo pobūdį gali viršyti tai, ko reikia norint parduoti produktą ar sutekti paslaugą. Neretai dirbtiniu intelektu renkami itin dideli duomenų kiekiai, jie analizuojami ir pertvarkomi, todėl gali būti sunku įrodyti, kad dirbtiniu intelektu pagrįsta analizė yra būtina sutarčiai įvykdyti (Information Commissioner's Office, 2017, p. 30). Atsižvelgiant į sunkumus, susijusius su duomenų tvarkymu sutikimo ar sutarties su duomenų subjektu pagrindu, teisėti duomenų valdytojo ar trečiosios šalies interesai kaip teisėtas teisinis pagrindas, laikomas alternatyviu pagrindu leidžiančiu išlaikyti pusiausvyrą tarp komercinės naudos naudojant dirbtinį intelektą bei

duomenų subjekto teisių (Information Commissioner's Office, 2017, p. 34-35). Aptariamu pagrindu duomenų tvarkymas yra teisėtas, kai duomenys tvarkyti yra būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, jei duomenų subjekto pagrindinės teisės ir laisvės nėra viršesnės už minėtų subjektų interesus (Europos Sąjungos Teisingumo Teismo 2017 m. gegužės 4 d. sprendimas *Rīgas satiksme*). Tai reiškia, kai asmens duomenų tvarkymui yra pasitelkiamas dirbtinis intelektas, duomenų valdytojas turi nustatyti vertybių sistemą, pagal kurią būtų galima patikrinti pasirinktą duomenų tvarkymą ir paaiškinti, kokie konkrečiai yra teisėti interesai. Vis dėlto, duomenų valdytojams gali būti neaišku dėl to, kokiu išsamumu turėtų būti pagrįstas teisėtas duomenų tvarkymo pagrindas, kai asmens duomenys yra tvarkomi naudojant dirbtinį intelektą, kuris neretai asmens duomenis tvarko dideliu mastu iš įvairių objektų teikiančių duomenis (Centre for Information Policy Leadership, 2018, p. 17).

Sąžiningumas yra ganėtini miglota ir bendro pobūdžio, bet kartu ir pagrindinė sąvoka, nustatantis pagrindinius duomenų apsaugos teisės principus (Kuner *et al.*, 2021, p. 68). Duomenų apsaugos teisės srityje sąžiningumo principo turinys nėra oficialiai apibrėžtas, todėl tai, ar duomenys yra tvarkomi sąžiningai, turi būti vertinama kiekvienu konkrečiu atveju, atsižvelgiant į faktines aplinkybes (Zaleskis, 2019, p. 114). Duomenų apsaugos teisėje sąžiningumo principas yra siejamas su duomenų valdytojų pareiga informuoti duomenų subjektus, kad jie tvarkys asmens duomenis teisėtai ir skaidriai, ir gebės įrodyti, kad duomenų tvarkymas atitinka BDAR reikalavimus (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 122). Konkrečiai, sąžiningumo principas lemia, kad duomenų valdytojas, tvarkydamas asmens duomenis, privalo atsižvelgti į duomenų subjekto interesus ir teisėtus lūkesčius (Zaleskis, 2019, p. 115). Atitinkamai, sąžiningumo principas gali būti įgyvendinamas užtikrinant (1) duomenų subjektų savarankiškumą (t. y. suteikiant duomenų subjektui kuo daugiau galimybių priimti sprendimu dėl jų asmens duomenų naudojimo, tvarkymo apimties ir sąlygų), (2) duomenų subjektų teisėtus lūkesčius (t. y. užtikrinant, kad tvarkant asmens duomenis bus išvengiama diskriminacinio poveikio dėl rasės, etninės kilmės, politinių pažiūrų, religijos, tikėjimo, priklausymo profesinei sąjungai, genetinės arba sveikatos būklės ar seksualinės orientacijos arba tokį poveikį turinčių priemonių atsiradimo (BDAR 71 konstatuojamoji dalis), be kita ko, (3) žmogaus įsikišimą, kuris reiškia, kad duomenų valdytojas turi pareigą užtikrinti kvalifikuotų asmens įsitraukimą tvarkant asmens duomenis (Europos duomenų apsaugos valdyba, 2020b, p. 19).

Sąžiningumo principo įgyvendinimas dirbtinio intelekto kontekste kelia iššūkių, kai siekiama užtikrinti duomenų subjekto (1) savarankiškumą; (2) teisėtus lūkesčius bei

(3) poreikį, kad į dirbtinio intelekto naudojime dalyvautų žmogaus. Visų pirma, siekiant užtikrinti duomenų subjekto savarankiškumą, Europos Sąjungos Komisija pabrėžia, kad fiziniams asmenims turėtų būti teikiama aiški informacija apie dirbtiniu intelektu pagrįstų sistemų naudojimą (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018). Tai reiškia, kad duomenų subjektas turėtų būti informuotas apie dirbtinio intelekto programų naudojimą, jų sistemos aprašymus, charakteristikas (Europos Komisijos Komunikatas Dirbtinis intelektas Europai, 2018) arba suteikta galimybė susipažinti su dirbtinio intelekto algoritmų struktūra ir, jei taikoma, su duomenų rinkiniais, naudojamais algoritmams apmokyti (Artificial Intelligence and Data Protection:.., 2019 p. 12). Tokios informacijos suteikimas būtinas siekiant užtikrinti, kad duomenų subjektas žinotų, kad jis sąveikauja su dirbtinu intelektu ir jo asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą. Tik aiškios ir tikslios informacijos suteikimas apie dirbtinio intelekto naudojimą asmens duomenų tvarkymui, gali užtikrinti galimybę duomenų subjektams kontroliuoti duomenis, kurie yra renkami dirbtinio intelekto ir laisva valia nuspręsti dėl duomenų tvarkymo apimties ar sąlygų. Vis dėlto, Europos Sąjungoje yra išreikštas susirūpinimas, kad dirbtinis intelektas gali būti neaiškus fiziniams asmenims. Pastebima, kad daugeliu atveju asmenys nežino, kada dirbtinis intelektas yra pasitelkiamas ir kokia apimtimi jis tvarko informaciją (Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos, 2019). Tai suponuoja išvadą, kad jei asmuo neišmano, kada dirbtinis intelektas yra naudojamas asmens duomenų tvarkymu, tinkamai nėra užtikrinamas duomenų subjekto savarankiškumas, kaip vienas iš sąžiningumo principo elementų. Antra, sąžiningumo principas yra neatsiejamas nuo teisėtų duomenų subjektų lūkesčių, kurių užtikrinimas gali būti kontroversiškas dėl dirbtinio intelekto šališkumo. Neretai įsivaizduojama, kad dirbtinis intelektas gali atlikti objektyvesnę analizę negu fizinis asmuo. Juk dirbtinio intelekto neveikia sumažėjęs cukraus kiekis kraujyje ar subjektyvus noras padėti draugui (Norwegian Data Protection Authority, 2018, p. 16). Tačiau Europos Sąjungos Parlamentas yra išreiškęs susirūpinimą dėl dirbtinio intelekto galimo šališkumo (Europos Parlamento rezoliucijos dėl visapusiškos Europos pramonės politikos dirbtinio..., 2019). Pabrėžiama, kad dirbtinis intelektas gali sukurti ar net sustiprinti šališkumą, priklausomai nuo to, kaip jis yra kuriamas ir naudojamas. Šališkumas gali atsirasti dėl duomenų rinkinių (Crawford *et al.*, 2017, p. 16-17), bet taip pat ir dėl tyčinių ar netyčinių dirbtinio intelekto kūrėjų veiksmų, t. y. dirbtino intelekto pagrįstus sprendimus riboja dirbtinio intelekto kūrėjų suvokimas apie pasaulį (Guidelines on artificial intelligence and..., 2019, p. 31). Be to, ne visada yra įmanoma visiškai panaikinti dirbtinio intelekto algoritmų šališkumą, nes idealų tikslą – gauti duomenis be klaidų – pasiekti gali būti sudėtinga, nes net ir išbandyta dirbtinio

intelekto sistema neišvengiamai susidurs su realaus pasaulio scenarijais, kurie gali lemti šališkus rezultatus, kai ji bus naudojama aplinkoje, kuri skiriasi nuo dirbtino intelekto sistemos mokymosi ir testavimo aplinkos. Paminėtinas dirbtinio intelekto šališkumą pagrindžiantis pavyzdys, kai elektroninės komercinės bendrovė „Amazon“ bandė naudoti įdarbinimo sistemą, grindžiamą dirbtiniu intelektu. Tačiau dirbtinio intelekto įsidarbinimo sistema suteikė didesnę galimybę įsidarbinti vyrams nei moterims dėl to, kad duomenys buvo surinkti iš įmonėje dirbančių darbuotojų, kurių didžiąją dalį sudarė vyrai (What the GDPR Shows Us..., 2023). Tai suponuoja, kad dirbtinis intelektas negali užtikrinti visiško objektyvo, o tai gali turėti įtakos duomenų rinkinių šališkumui ir lemti dirbtinio intelekto priimtų sprendimų diskriminacinį pobūdį (Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir..., 2020). Atitinkamai, toks netikslus asmens duomenų tvarkymas pasitelkiant dirbtinį intelektą, neatitinka teisėtų duomenų subjekto lūkesčių, kad asmens duomenys bus tvarkomi išvengiant bet kokio diskriminacinio pobūdžio. Tokiu atveju, manytina, jei įtariama, kad duomenų tvarkymas, pagrįstas dirbtiniu intelektu gali sukelti diskriminacinį rezultatą, turėtų būti atliekami dirbtinio intelekto tyrimai, kurie apimtų informacijos, pagal kurią grindžiama asmens duomenų atranka, peržiūrą ir algoritmo kūrimo būdo patikrinimą. Trečia, siekiant tinkamai įgyvendinti sąžiningumo principą, duomenų tvarkymas turėtų būti siejamas su duomenų valdytojų pareiga užtikrinti kvalifikuotą žmogaus įsikišimą, galintį atskleisti šališkumus, kuriuos gali sukurti technologijos (Europos duomenų apsaugos valdyba, 2020, p. 19). Dirbtinio intelekto naudojime, Europos Sąjunga pabrėžia, kad dirbtinis intelektas yra ne tik orientuotas į žmogų, žmogaus sukurtas, bet ir žmogaus kontroliuojamas (Aukšto lygio ekspertų grupė dirbtinio..., 2019b, p. 4). Todėl naudojant dirbtinį intelektą ir juo priimant sprendimus, turi būti taikoma žmogaus priežiūra, įsikišimas ir kontrolė, kad bet kuriuo metu dirbtinio intelekto naudotojai galėtų sustabdyti ar pakeisti dirbtinio intelekto atliekamas funkcijas (Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių..., 2020). Aktualu, kad duomenų valdytojai pasitelktų kvalifikuotus subjektus, kurie galėtų užtikrinti, kad asmens duomenys būtų tvarkomi teisėtai dirbtinio intelektų sistemų (pvz., atliekant techninę priežiūrą, taisymus, tobulinimus ar programinės įrangos atnaujinimus) (Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir..., 2020). Kitu atveju, be kvalifikuoto asmens įsikišimo, tvarkant asmens duomenis, pasitelkus dirbtinį intelektą, išlieka rizika, kad asmens duomenys bus netikslūs.

Skaidrumo principas apima kelis aspektus: (1) duomenų tvarkymas turi būti skaidrus duomenų subjektų atžvilgiu; (2) duomenų tvarkymas turi būti skaidrus priežiūros

institucijos, kuri atlieka duomenų valdytojo priežiūrą, atžvilgiu (Zaleskis, 2019, p. 166). Analizuojant duomenų tvarkymo skaidrumą duomenų subjektu atžvilgiu, BDAR 39 konstatuojamojoje dalyje detalizuojamas skaidrumo principas nurodant, kad fiziniams asmenims turi būti aišku, kaip jų asmens duomenys yra renkami, naudojami arba kokiu mastu duomenys yra tvarkomi. Detalizuojant duomenų subjektams teikiamos informacijos kokybę, 29 straipsnio duomenų apsaugos darbo grupė yra nurodžiusi, kad informacija duomenų subjektui turi būti turi būti pateikiama glausta, skaidria, suprantama, lengvai prieinama forma ir aiškia, paprasta kalba (29 straipsnio duomenų apsaugos darbo grupė, 2017a, p. 7). Tai reiškia, kad skaidrumo principu yra užtikrinama duomenų subjektų teisė būti informuotam apie duomenų tvarkymą (BDAR 13-14 straipsniai). Atitinkamai, skaidrumo principas įtvirtina reikalavimą, kad duomenų subjektui būtų aišku, kaip su juo susiję asmens duomenys yra renkami ir naudojami, be kita ko, kaip su jais galima susipažinti, kaip jie yra tvarkomi ar bus tvarkomi (Zaleskis, 2019, p. 116). Skaidrumas aktualus ir priežiūros institucijų atžvilgiu. Tai reiškia, kad duomenų valdytojas ir duomenų tvarkytojas turi pareigą bendradarbiauti su priežiūros institucijomis. Šią pareigą privalo įgyvendinti gavę prašymą. Prašymo pagrindu, duomenų valdytojas, duomenų tvarkytojas arba jų atstovas, turėtų pateikti duomenų tvarkymo veiklos įrašus priežiūros institucijai (Zaleskis, 2019, p. 117).

Dirbtiniu intelektu pagrįsto duomenų tvarkymo atveju skaidrumo principas yra aktualaus, nes minėtas principas turi sudaryti sąlygas duomenų subjektams būti informuotiems apie duomenų tvarkymą. Ši informacija turi būti lengvai prieinama, pateikta aiškia ir suprantama kalba (Agencia Española Protección Datos, 2020, p. 31). Tačiau skaidrumo principo užtikrinimas, kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą yra sudėtingas. Taip yra dėl to, kad visų pirma, itin didelį duomenų kiekį generuojanti ir savaime besimokanti dirbtino intelekto prigimtis, manytina, prieštarauja bandymas suteikti duomenų subjektams aiškią informaciją apie duomenų tvarkymą (Mitrou, 2019, p. 58). Norvegijos duomenų apsaugos tarnyba yra pabrėžusi, kad yra sudėtinga įgyvendinti skaidrumo principą, nes kuriant ir naudojant dirbtinį intelektą yra sunku suprasti ir paaiškinti, kaip informacija yra susieta, ir kaip įvertinta konkrečiame procese (Norwegian Data Protection Authority, 2018, p. 19). Antra, dirbtinis intelektas yra susijęs su „juodosios dėžės“ problematika. „Juodosios dėžės“ problematika reiškia, kad dirbtinis intelektas remiasi mašininio ir giliojo mokymosi algoritmais, kurie renka, naudoja ir tvarko asmens duomenis taip, kad duomenų subjektui nėra paprasta juos suprasti (Bathaee , 2018, p. 901). Dėl minėto dirbtinio intelekto renkamo didelio asmens duomenų kiekio ir procesų sudėtingumo, duomenų valdytojas neretai gali nežinoti, kaip tinkamai

informuoti duomenų subjektą apie tvarkomus asmens duomenis ir kaip informaciją pateikti lengvai prieinama, aiškia ir suprantama kalba. Rezultate, duomenų subjektas gali būti tinkamai neinformuotas, kokie duomenys yra renkami (pvz., jo mobiliojo telefono buvimo vieta), kaip jie yra apdorojami (pvz., kaip jų paieškos rezultatai yra filtruojami) arba kaip yra priimami sprendimai (pvz., naudojamasi socialinėse medijose paskelbtais duomenis, kad būtų įvertintas asmens kreditingumas) (Information Commissioner's Office, 2017, p. 27). Tai suponuoja skaidrumo principo neįgyvendinimą, nes duomenų subjektui nebus pateikta tinkama informacija apie duomenų rinkimą ir bus priimti sprendimai duomenų subjektų atžvilgiu, kurių jie nesupranta ir negali kontroliuoti (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 45). Šiai problemai spręsti, Prancūzijos duomenų apsaugos tarnyba rekomenduoja siekti suprasti bendrą dirbtinio intelekto logiką ir teikti prioritetą ne techniniam procesų aprašymui. Tokia pozicija reiškia, kad dirbtinio intelekto naudojimas asmens duomenų tvarkymui turėtų būti paaiškinamas žodžiais, o ne koduotėmis (Mitrou, 2019, p. 56-57).

Skaidrumo principo užtikrinimo problematiką dirbtinio intelekto kontekste pabrėžia ir Europos Sąjungos institucijos. Pavyzdžiui, Europos duomenų apsaugos valdyba ir Europos duomenų apsaugos priežiūros pareigūnas yra išreiškę nuomonę, kad dirbtinio intelekto skaidrumo užtikrinimas yra sudėtingas procesas (Europos duomenų apsaugos valdyba *et al.*, 2021, p. 19). Atitinkamai, Dirbtinio intelekto akte yra įtvirtinamas skaidrumo reikalavimas. Konkrečiai, Dirbtinio intelekto 13 straipsnyje 1 dalyje nustatyta didelės rizikos dirbtinio intelekto sistemų tiekėjų skaidrumo reikalavimas dirbtinio intelekto naudotojams, siekiant užtikrinti, kad dirbtinio intelekto sistemos veiktų skaidriai, kad naudotojai galėtų tinkamai interpretuoti ir naudoti sistemos išvedinius. Taip pat, Dirbtinio intelekto akto 13 straipsnio 2 dalyje reglamentuojama, kad su didelės rizikos dirbtinio intelekto sistemomis turėtų būti pateikiamos skaitmeninio ar kitokio formato instrukcijos, kuriuose turėtų būti pateikta glausta, išsami, teisinga ir aiški, naudotojams svarbi ir suprantama informacija. Yra nuomonių, kad minėto straipsnio reguliavimu galima užtikrinti platesnį dirbtinio intelekto suderinimą su BDAR, įskaitant ir skaidrumo principu (Vale, 2022). Vis dėlto, Dirbtinio intelekto aktas konkrečiai nedetalizuoja, ar minėtas skaidrumo reikalavimai turėtų būti taikomas ir naudojant dirbtinį intelektą asmens duomenų tvarkymui. Tik Dirbtinio intelekto akto aiškinamajame memorandume pastebima, kad Dirbtinio intelekto akto pasiūlymas nedaro poveikio BDAR, tačiau tai neužtikrina teisinio aiškumo, ar Dirbtinio intelekto aktu įtvirtinti skaidrumo reikalavimai galėtų papildyti BDAR įtvirtintą skaidrumo principą.

Taigi, teisėtumo, sąžiningumo ir skaidrumo principai yra fundamentalūs dirbtinio intelekto kūrimui ir naudojimui, kai atliekamas asmens duomenų tvarkymas. Teisėtumo principas aktualus siekiant pasirinkti teisėtą duomenų tvarkymo pagrindą, kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą, tačiau ši principą įgyvendinti duomenų valdytojams gali būti sudėtinga dėl dirbtinio intelekto specifikos, kuri yra pagrįsta didelius duomenų kiekių rinkimu įvairiais tikslai. Sąžiningumo principas yra neatsiejamas nuo teisėtų duomenų subjekto interesų ir lūkesčių, kurie gali būti neužtikrinti, jei duomenų subjektas aiškiai nežino, kada duomenų tvarkymui yra naudojamas dirbintis intelektas, neužkertamas galimas dirbtinio intelekto šališkumas ir kvalifikuoto asmens įsikišimas. Skaidrumo principu užtikrinamas duomenų subjektų informavimas apie duomenų tvarkymą, tačiau dirbtinio intelekto kontekste šio principo įgyvendinimas yra sudėtingas, nes kuriant ir naudojant dirbtinį intelektą yra sudėtinga paaiškinti, kaip informacija yra susiejama, o „juodosios dėžės“ problematika kelia iššūkių duomenų subjektams siekiant suprasti, kaip asmens duomenys yra tvarkomi dirbtinio intelekto.

3.2. Duomenų tvarkymo tikslo apribojimo principas

BDAR 5 straipsnio 1 dalies b punktas apibrėžia sąžiningumo principo nulemtą (Zaleskis, 2019, p. 166) duomenų tvarkymo tikslo apribojimo principą, pagal kurį reikalaujama, kad (1) asmens duomenys būtų renkami konkrečiais, aiškiai apibrėžtais ir teisėtais tikslais (tikslo nurodymo aspektas) (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 11-12); (2) ir toliau nebūtų tvarkomi su tais tikslais nesuderinamu būdu (suderinamo naudojimo aspektas) (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 12-13).

Tikslo nurodymo aspektas reiškia, kad duomenys yra renkami tam tikriems tikslams ir šie tikslai yra duomenų tvarkymo esmė (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 15). Europos Sąjungos *soft law* praktikoje tikslo nurodymo aspektas kelia tris sąlygas: (1) duomenų tvarkymo tikslas turi būti konkretus; (2) duomenų tvarkymo tikslas turi būti aiškus; (3) duomenų tvarkymo tikslas turi būti teisėtas (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 15). Pirmoji sąlyga reiškia, kad ne vėliau kaip iki asmens duomenų rinkimo pradžios, asmens duomenų tvarkymo tikslai turi būti išsamiai identifikuoti (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 39). Kitu atveju, kai asmens duomenys yra tvarkomi neapibrėžtais, neribotais tikslais ir neribota apimtimi, toks duomenų tvarkymas neatitinka konkretumo reikalavimo (Kuner *et al.*, 2020, p. 315). Antroji sąlyga reiškia, kad duomenų tvarkymo tikslai turi būti nedviprasmiški (Kuner *et al.*, 2020, p. 316), atskleisti, paaiškinti ir išreikšti suprantama forma (Zaleskis, 2019, p. 119),

kad kiekvienas asmuo suprastų asmens duomenų tvarkymo tikslus (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 39). Aiškiai apibrėžti duomenų tvarkymo tikslai turi būti atskleisti duomenų subjektui teikiamoje informacijoje, duomenų tvarkymo veiklos įrašuose, poveikio duomenų apsaugai vertinime ar sutartyje (Zaleskis, 2019, p. 119). Galiausiai, trečioji sąlyga detalizuoja teisėtumo principą (Zaleskis, 2019, p. 119) ir priklauso nuo aplinkybių, nes siekiama, kad kiekvienu atveju būtų užtikrinta visų suinteresuotų asmens teisių, laisvių ir interesų apsauga ir nebūtų taikomi neproporcingi apribojimai vardan duomenų valdytojo interesų (Boulanger *et al.,* 1997 cituota Kuner *et al.,* 2020, p. 315). Visais atvejais duomenų tvarkymas, kuriuo siekiama neteisėto tikslo (t. y. prieštaraujančio tarptautinės, Europos Sąjungos, nacionalinės teisės aktams), negali būti laikomas pagrįstu teisėtu tikslu (Kuner *et al.,* 2020, p. 315).

Dirbtinio intelekto naudojimui tvarkant asmens duomenis, konkretaus, aiškaus ir teisėto tikslo apsibrėžimas yra svarbus, kad duomenų subjektas galėtų pasirinkti, ar sutinka su duomenų tvarkymu (How to Train an AI, 2022) ir siekiant nustatyti, ar dirbtinis intelektas yra naudojamas atitinkant teisės aktų reikalavimus (Conrad, 2017 cituota Mitrou, 2019, p. 47). Pavyzdžiui, specialiojoje literatūroje yra nurodoma, kad siekiant užtikrinti duomenų tvarkymo tikslo apribojimo principo įgyvendinimą, yra draudžiama naudoti „Siri“ ar „Alexa“ siekiant atlikti asmenų balsų analizę ir gauti biometrinių duomenų išvadas, o sveikatingumo sekimo prietaisus naudoti siūlant maistinius preparatus ar vaistus (Mitrou, 2019, p. 47). Vis dėlto, dirbtinis intelektas yra pagrįstas algoritmų naudojimu, o mašininis ir gilusis mokymasis skatina dirbtinį intelektą rinkti kuo daugiau duomenų, generuoti naujus duomenis ir naujas duomenų rūšis (Information Commissioner’s Office, 2017, p. 19). Todėl reikalavimas iš anksto apibrėžti duomenų tvarkymo tikslą prieštarauja dirbtinio intelekto koncepcijai, pagal kurią dirbtinis intelektas turi vystytis savarankiškai, mokydamasis iš didžiųjų duomenų, neapibrėžtais tikslais (Purtova, 2018, p. 56). Neretai dirbtiniu intelektu grįstos sistemos, kurios tvarko asmens duomenis duomenų tvarkymo tikslą apibrėžia itin abstrakčiai. Pavyzdžiui, „Google“ informuoja duomenų subjektus, kad naudoja automatines sistemas, kurios analizuoja turinį ir renka duomenis siekiant teikti rekomendacijas, personalizuotą turinį ir pritaikytus paieškos rezultatus (Why Google collects data, 2022). „Facebook“ taip pat nustato itin platų duomenų tvarkymo tikslą, nurodant, kad asmens duomenys yra tvarkomi siekiant teikti „Facebook“ produktus, įskaitant turinio personalizavimą ar pasiūlymų teikimą produktuose (Privacy Policy. What is the..., 2023). 29 straipsnio duomenų apsaugos darbo grupė nuomone, duomenų tvarkymo tikslas negali būti bendras (pvz., „naudotojo patirties gerinimui“) (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 16). Minėta išvada yra svarbi, nes minėtais „Google“ ir

„Facebook“ pavyzdžiais naudojami algoritmai apdoroja asmens duomenis, siekiant pagerinti teikiamą paslaugą ar produktą. Visgi, duomenų tvarkymo tikslo apribojimų nustatymas gali kelti grėsmę, kad bus užkirstas kelias vystyti dirbtinio intelekto technologijas ir išnaudoti jų potencialą (Wallace *et al.*, 2018, p. 14), todėl yra sudėtinga rasti tinkamą pusiausvyrą tarp duomenų tvarkymo tikslų apribojimo principo ir dirbtinio intelekto technologijų naujovių. Daugelyje dirbtinio intelekto naudojimo atvejų yra praktiškai neįmanoma numatyti, ką algoritmas išmoks. Be to, tikslas gali keistis savaime besimokančio dirbtinio intelekto vystymosi eigoje, ypač dėl to, kad atitinkami duomenų tvarkymo tikslai gali būti nežinomi duomenų rinkimo metu (Paal, 2022, p. 294). Atitinkamai, teigtina, kad dirbtinis intelektas yra neatsiejamas nuo naujų asmens duomenų kiekio generavimo, kurie neretai yra renkami, tvarkomi ir naudojami neapibrėžtais tikslais.

Suderinamumo naudojimo aspektas riboja tolesnį duomenų tvarkymą su pirminiais duomenų tvarkymo nesuderinamais būdais (29 straipsnio duomenų apsaugos darbo grupė, 2013, p. 13). Dirbtinis intelektas, kuris yra pagrįstas dideliais duomenimis gali asmens duomenis naudoti kitiems tikslams nei iš pradžių jie buvo surinkti ir bet kokia surinkta informacija gali būti vertinama iš naujo (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 362-363). Todėl kuriant ir naudojant dirbtinį intelektą susiduriama su iššūkiu, susijusiu su tuo, kad dirbtinio intelekto funkcionavimui neretai reikia daug skirtingų rūšių asmens duomenų, įskaitant ir informaciją, kuri buvo surinkta kitais tikslais. Pavyzdžiui, siekiant pagerinti balsų valdomų prietaisų veikimą, gali būti renkami asmens kalbos įrašai. Šie įrašai gali būti naudojami algoritmams, kuriais siekiama nuspėti informaciją apie kalbančiojo sveikatą, mokyti. Toks pakartotinis informacijos panaudojimas gali būti naudingas ir padėti atlikti tikslesnes analizes nei tos, kurios buvo techniškai įmanomos anksčiau (International Working Group on Data Protection in Telecommunications, 2018, p. 9). Toks antrinis duomenų rinkimas yra dirbtinio intelekto taikomų sistemų bruožas, kai yra renkami didieji duomenys, kurių analizė apima duomenų rinkimo paskirties keitimą, sudėtingą algoritmų taikymą ir išvadų apie duomenų subjektą darymą (Richards *et al.*, 2013). Nors tokios informacijos sisteminimas pasitelkiant dirbtinį intelektą, manytina, prieštarauja duomenų tvarkymo tikslumo apribojimo principui, tačiau nėra nuoseklios pozicijos, kaip turėtų būti vertinamas toks dirbtiniu intelektu pagrįstas antrinis duomenų rinkimas kitu tikslu nei tuo, kuriuo jie buvo surinkti. Pavyzdžiui, Jungtinės Karalystės informacijos tarnybos nuomone, duomenų tvarkymo tikslo apribojimo principas neturėtų būti neįveikiama kliūtis pakartotiniams asmens duomenis išgauti (Information Commissioner’s Office (2017) cituota Butterworth, 2018, p. 260). Tam tikras pakartotinis duomenų naudojimas gali būti laikomas suderintu su pirminiais

duomenų tvarkymo tikslais, jei jis atliekamas viešojo intereso labui, mokslinių ar istorinių tyrimų ar statistiniais tikslais (BDAR 5 straipsnio 1 dalies b punktas). Tai reiškia, kad duomenų tvarkymu mokslinių tyrimų tikslais siekiama informacijos, kuri gali padėti suprasti įvairių mokslo sričių reiškinius (pvz., epidemiologijos, kriminologijos ir pan.) (Kuner *et al.*, 2020, p. 316). Atitinkamai, kyla klausimas, kas yra mokslinis tyrimas ir kokiu mastu dirbtinio intelekto kūrimas ir taikymas yra mokslinis tyrimas. BDAR neapibrėžta, kas yra mokslinis tyrimas. BDAR 159 konstatuojamojoje dalyje tik abstrakčiai nurodoma, kad moksliniai tyrimai turėtų būti aiškinami plačiai ir apimti technologinę plėtrą, ir demonstravimą, fundamentinius mokslinius tyrimus, taip pat taikomuosius, ir privačiai finansuojamus mokslinius tyrimus. Vis dėlto, tai nepaaiškina, ar moksliniu tyrimu turėtų būti laikomas dirbtinio intelekto kūrimas ir taikymas, kurio pasitelkiami dideli kiekiai asmens duomenų. Norvegijos duomenų apsaugos tarnybos nuomone yra sudėtinga atskirti dirbtinio intelekto kūrimą ir taikymą, nes dirbtinio intelekto kategorijos nuolat yra vystomos ir tobulėja, todėl neaišku, kur baigiasi moksliniai tyrimai ir prasideda dirbtinio intelekto naudojimas (Norwegian Data Protection Authority, 2018, p. 18). Todėl iki šiol nėra pripažintos vieningos išvados, ar dirbtinio intelekto kūrimas ir taikymas, yra mokslinis tyrimas, ar ne.

Vadinasi, tikslo apribojimo principas yra susijęs su reikalavimu nurodyti duomenų tvarkymo tikslą ir užtikrinti su pirminiais tikslais suderinamą duomenų tvarkymą. Šio principo įgyvendinimas dirbtino intelekto kontekste kelia iššūkių, nes dirbtinis intelektas yra pagrįstas didelių ir naujų asmens duomenų kiekių generavimu, kurie neretai renkami ir tvarkomi neapibrėžtais tikslais. Tolimesnio duomenų tvarkymo suderinimas su pirminiais duomenų tvarkymo tikslais dirbtinio intelekto kontekste yra sudėtingas, nes dirbtinio intelekto vystymuisi ir funkcionavimui reikia skirtingų rūšių asmens duomenų, įskaitant, asmens duomenų, kurie yra surinkti kitais tikslais nei iš pradžių jie buvo renkami.

3.3. Duomenų kiekio mažinimo principas

Tarptautinių teisės šaltiniai skirtingai reglamentuoja duomenų kiekio mažinimo principo apimtį. Pavyzdžiui, Europos Tarybos duomenų apsaugos konvencijos 5 straipsnio 1 dalies c punkte nustatyta, kad automatizuotai tvarkomi asmens duomenys turi būti: „tinkami, svarbūs ir ne pernelyg didelės apimties, kurie atitinka konkrečius tikslus“, o EBPO privatumo gairių 8 straipsnyje nustatyta, kad „duomenys turi būti būtini“. Tuo tarpu, BDAR 5 straipsnio 1 dalies c punkte nustatyta, kad „asmens duomenys turi būti: adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi“.

Duomenų kiekio mažinimo principas aiškinamas, nurodant, kad asmens duomenys turi būti (1) neperteklinia, (2) tinkami ir (3) adekvatūs (Kuner *et al.*, 2020, p. 317). Visų pirma, duomenų kiekio mažinimo principas siejamas su neperteklinių duomenų naudojimu (Kuner *et al.*, 2021, p. 68), kuris reiškia, kad asmens duomenys turi būti tvarkomi tik tuo atveju, jei tikslų negalima pagrįstai pasiekti kitomis priemonėmis (BDAR 39 konstatuojamoji dalis). Be to, šis būtinumo reikalavimas susijęs ne tik su asmens duomenų kiekiu, bet ir duomenų kokybe (Kuner *et al.*, 2020, p. 317). Antra, tinkamumo reikalavimas reikalauja, kad duomenų valdytojas įsivertintų, ar asmens duomenys yra reikšmingi duomenų tvarkymo tikslais (Europos duomenų apsaugos valdyba, 2020b, p. 74). Trečia, remiantis adekvatumo reikalavimu, duomenų valdytojas turi patikrinti, ar atitinkami tikslai gali būti pasiekti tvarkant minimalų kiekį asmens duomenų (Lietuvos vyriausio administracinio teismo 2012 m. gruodžio 18 d. sprendimas administracinėje byloje), ar apskritai netvarkant asmens duomenų (Europos duomenų apsaugos valdyba, 2020b, p. 21).

Nagrinėjant duomenų kiekio mažinimo principą dirbtinio intelekto kontekste, atkreiptinas dėmesys, kad duomenų kiekio mažinimo principas yra glaudžiai susijęs su duomenų tvarkymo tikslo apribojimo principu, nes nenustačius aiškiai apibrėžtų ir teisėtų duomenų tvarkymo tikslų yra neįmanoma užtikrinti, kad asmens duomenys yra tinkami, susiję su tikslais ir ribojami pagal tai, kiek jų reikia atsižvelgiant į tikslus, kuriais jie tvarkomi (GDPRHub, 2023). Tai reiškia, kad jei asmens duomenų tvarkymas atitinka duomenų tvarkymo tikslo apribojimo principo, jis taip pat atitiks ir duomenų kiekio mažinimo principą (Butterworth, 2018, p. 260). Tačiau kaip buvo minėta anksčiau, duomenų valdytojams, kurie pasitelkia dirbtinį intelektą asmens duomenų tvarkymui tenka iššūkis nustatyti duomenų tvarkymo tikslus, turint omenyje, kad neretai yra sudėtinga identifikuoti, ką dirbtinis intelektas išmoks. Tai suponuoja, kad duomenų valdytojams, kurie tvarko asmens duomenis naudodami dirbtinį intelektą, kuris pasižymi dideliu duomenų kiekių rinkimu (Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos, 2019) yra komplikuota apibrėžti duomenis, kurie yra reikalingi pagal duomenų kiekio mažinimo principą (Norwegian Data Protection Authority, 2018, p. 18). Mokslinėje literatūroje yra nuomonių, kad duomenų kiekio mažinimo principas tiesiogiai prieštarauja dirbtinio intelekto koncepcijai (Centre for Information Policy Leadership, 2018, p. 19). Toks požiūris grindžiamas dirbtinio intelekto taikomų sistemų pobūdžiu, dėl kurių neretai yra sudėtinga nustatyti, kokio asmens duomenų kiekio reikia, kad dirbtinis intelektas galėtų priimti sprendimą (Paal, 2022, p. 295-296). Atitinkamai, užtikrinti, kad asmens duomenys būtų neperteklinia dirbtinio intelekto naudojime yra sudėtinga atsižvelgiant į tai, kad asmens duomenys tapo komerciniu objektu ir duomenų valdytojai

yra suinteresuoti kaupti kuo duomenų, siekiant plėtoti teikiamą paslaugą ar produktą. Šis procesas neretai dar vadinamas „duomenų maksimizavimu“, kurio esmė yra analizuoti didžiulius duomenų kiekius, siekiant surasti naujų sąsajų tarp duomenų ir pateikti tikslesnes prognozes (International Working Group on Data Protection in Telecommunications, 2018, p. 9). Be to, kaip buvo minėta, dirbtiniam intelektui kurti reikia didžiųjų duomenų (angl. *big data*), t. y. didelių duomenų kiekių, kurie yra sukuriami žmonių ar mašinų (pvz., pirkimo sandorių duomenų, naudojimosi socialiniais tinklais įpročių ir pomėgių). Europos Sąjungos pagrindinių teisių agentūra yra nurodžiusi, kad didieji duomenys yra duomenų kiekio mažinimo principo antitezė (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 368). Sutiktina su tokiu požiūriu, nes didieji duomenys renka ir analizuoja kuo daugiau duomenų, o daugeliu atvejų – visus tam tikros aibės duomenis, o ne imtis (Information Commissioner’s Office, 2017, p. 40-41). Teigtina, kad, didieji duomenys kelia pavojų duomenų kiekio mažinimo principui, nes didžiųjų duomenų taikomosios programos paprastai renka duomenis iš įvairių šaltinių. Atitinkamai, gal kilti klausimas, ar surinkti duomenys yra tinkami ir adekvatūs (pvz., atliekant didžiųjų duomenų analizę gali būti aptiktos koreliacijos tarp duomenų apie asmens gyvenimo būdą ir jo kreditingumą, tačiau tai nereiškia, kad bet kokia informacija, kurią apie juos galima gauti, būtinai yra svarbi kredito rizikai įvertinti) (Information Commissioner’s Office, 2017, p. 40-41). Nepaisant duomenų kiekio mažinimo principo ir dirbtinio intelekto, pagrįsto didžiaisiais duomenimis, neatitikties, rekomenduoja kuriant naujas technologijas, minėtą principą taikyti lanksčiai. Tokį požiūrį patvirtina veido atpažinimo programinę įrangą kuriantys mokslininkai, kurie nustatė, kad didelė prieiga prie asmens duomenų (pvz., net asmens kilmės, rasės ar etninės priklausomybės), užtikrina veido atpažinimo sistemos tikslumą ir mažina dirbtinio intelekto šališkumą (Roach, 2018).

Apibendrinant, galima teigti, kad pagal duomenų kiekio mažinimo principas, dirbtinio intelekto sistemos asmens duomenis turėtų tvarkyti neperteklinias, tinkamais ir adekvačiais tikslais, tačiau dirbtinis intelektas yra neatsiejamas nuo „duomenų maksimizavimo“ ir didžiųjų duomenų, kurie yra reikalingi dirbtinio intelekto vystymuisi ir tinkamam funkcionavimui.

3.4. Duomenų tikslumo principas

Reikalavimas, kad duomenys būtų tikslūs yra nustatyti tiek Europos Tarybos duomenų apsaugos konvencijos 5 straipsnio d punkte, tiek EBPO privatumo gairių 8 straipsnį. BDAR duomenų tikslumo principą įtvirtina 5 straipsnio 1 dalies d punkte, nustatydamas, kad

„asmens duomenys turi būti: tikslūs ir prireikus atnaujinami. Duomenų valdytojai yra įpareigojami imtis visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, būtų nedelsiant ištrinami arba ištaisomi“.

BDAR nereglamentuoja, kokie duomenys yra laikomi tiksliais (Zaleskis, 2019, p. 124). Duomenys gali apimti tiek subjektyvią (pvz., trečiųjų asmenų nuomonę apie duomenų subjektą), tiek objektyvią (pvz., asmens vardą, pavardę, gimimo datą) informaciją (GDPRHub, 2023). Subjektyvios informacijos tikslumo neįmanoma nustatyti, todėl jai netaikomas duomenų tikslumo principas. Tuo tarpu, objektyvi informacija gali būti patikrinta, todėl patenka į BDAR 5 straipsnio 1 dalies d punkto taikymo sritį (GDPRHub, 2023).

Tikslumo principas yra taikomas ne tik objektyviai informacijai, bet prognozėms (29 straipsnio duomenų apsaugos darbo grupė, 2017b, p. 12), o tai ypač aktualu dirbtiniu intelektu pagrįstam duomenų tvarkymui. Dirbtinio intelekto daromos prognozės gali būti objektyviai netikslios, jei jos grindžiamos neaktualia, neišsamia ar klaidinga informacija (Europos Parlamento rezoliucija dėl visapusiškos Europos pramonės politikos..., 2019) ar yra neteisingų išvadų rezultatas (Europos duomenų apsaugos valdyba, 2020b, p. 24-25). Akivaizdu, kad neteisingi ar neaktualūs duomenys, gali lemti įvairaus sunkumo klaidas arba sutrikimus, pavyzdžiui, tikslinės reklamos siuntimu, kuri neatitinka asmens profilio informacijos ar neteisingos medicininės diagnozės konstatavimu. Atitinkamai, dirbtinio intelekto sistemų įvesties duomenų kokybės užtikrinimas yra iššūkis, kuris tapus vis savarankiškesnėms dirbtinio intelekto sistemoms, taps vis svarbesnis (Demiaux *et al.*, 2017, p. 39-40). Daugeliu atveju dirbtinio intelekto prognozės gali būti netikslios tiek dėl duomenų, kurie yra sugadinti apčiuopiamo techninio gedimo, kurį sukelia duomenis renkantys jutikliai, tiek ir dėl žmogiškojo faktoriaus, kylančios dėl suinteresuotųjų asmenų šališkų duomenų įvesčių (Demiaux *et al.*, 2017, p. 40). Specialioje literatūroje teigiama, kad dirbtinis intelektas dėl tvarkomų didelių duomenų kiekių, gali toleruoti tam tikrą „netikslių“ duomenų kiekį (Information Commissioner’s Office, 2017, p. 43), nes tam tikras duomenų „netikslumas“ (pvz., neteisingas gyvenamosios vietos adresas) gali neturėti įtakos bendrosioms tendencijoms nustatyti (Information Commissioner’s Office, 2017, p. 44). Vis dėlto, manytina, kad duomenų tikslumo principo užtikrinimas yra sudėtingas duomenų valdytojams, kurie pasitelkia dirbtinį intelektą asmens duomenų tvarkymui, nes informacija yra renkama iš įvairių šaltinių ir nėra galimybės patikrinti, ir / arba išlaikyti surinktų duomenų tikslumą (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 368). Be to, BDAR netekia jokių privilegijų duomenų valdytojams minėto principo

taikymo aspektu. Priešingai, duomenų valdytojai yra atsakingi už tvarkomų asmens duomenų tikslumą, nepaisant, kokią technologiją jie naudoja.

Taigi, duomenų tikslumo principas nustato, kad asmens duomenys turi būti tikslūs ir prireikus atnaujinami, tačiau daugeliu atveju dirbtinio intelekto surinkti duomenys gali būti netikslūs dėl techninio gedimo ar subjektyvios įvesties klaidos, o asmens duomenų atnaujinimas kelia iššūkių duomenų valdytojams, kurie gali neturėti galimybės patikrinti ar išlaikyti surinktų duomenų tikslumą dėl dirbtiniam intelektui būdingo požymio didele apimtimi rinkti informaciją iš įvairių šaltinių.

3.5. Duomenų saugojimo trukmės apribojimo principas

Europos Tarybos duomenų apsaugos konvencijos 5 straipsnio 4 dalies e punktas ir BDAR 5 straipsnio 1 dalis e punktas įtvirtina duomenų saugojimo trukmės apribojimo principo sampratą, nustatančią, kad asmens duomenys turi būti laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi.

Duomenų saugojimo trukmės apribojimo principas yra susijęs su duomenų saugojimo laiku (Zaleskis, 2019, p. 127). BDAR konkretūs duomenų saugojimo terminai nėra nustatyti (Zaleskis, 2019, p. 127). BDAR 39 konstatuojamoje dalyje nustatoma, kad asmens duomenų saugojimo laikotarpis turėtų būti minimalus. Tai patvirtina ir Europos Sąjungos Teisingumo Teismo praktika, kurioje konstatuota, kad teisės aktai, kuriais nustatomas bendras ir beatodairiškas asmens duomenų saugojimas, peržengia griežtai būtino saugojimo ribas ir negali būti laikomi pateisinamais (Europos Sąjungos Teisingumo Teismo 2016 m. gruodžio 21 d. sprendimas *Tele2 Sverige*). Todėl jei duomenų valdytojui nebėra aktuali duomenų subjekto tapatybė, duomenys turėtų būti ištrinami arba nuasmeninami (Zaleskis, 2019, p. 127). Atitinkamai, duomenų valdytojas yra raginamas nustatyti duomenų ištrynimo arba periodinės peržiūros terminus, siekiant užtikrinti, kad asmens duomenys nebūtų saugomi ilgiau nei būtina (Kuner *et al.*, 2020, p. 318). Šiuo atveju reikėtų atsižvelgti į BDAR 25 straipsnio 2 dalį, kuriuo duomenų valdytojams nurodoma įgyvendinti tinkamas technines ir organizacines priemones, kuriomis būtų užtikrinama, kad laikomasi teisėto asmens duomenų saugojimo (Kuner *et al.*, 2020, p. 318).

Duomenų saugojimo trukmės apribojimo principas kelia iššūkių dirbtinio intelekto kontekste. Asmens duomenų ištrynimas ar apribojimas po to, kai jų paskirtis yra įvykdyta, gali trukdyti tiek dirbtinio intelekto technologijos kūrimui, tiek naudojimui (Paal, 2022, p. 295). Be to, duomenų saugojimo trukmės apribojimo principas gali būti neįgyvendintas,

kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą, nes visų pirma, pastebima tendencija, kad duomenų saugojimo pajėgumui nuolatos didėja, o jų saugojimo sąnaudos mažėja; antra, dirbtinis intelektas, kuris geba apdoroti didelius duomenų kiekius gali skatinti duomenų valdytoju saugoti duomenis ilgiau nei yra tikslinga (Information Commissioner's Office, 2017, p. 40). Be to, duomenų saugojimo trukmės apribojimo principo įgyvendinimas dirbtinio intelekto kontekste, gali skirtis priklausomai nuo srities, kurioje yra renkama informacija. Pavyzdžiui, klinikiniuose tyrimuose, asmens duomenys gali būti saugomi pagrįstai ilgesnį laikotarpį, tuo tarpu, privačios įmonės, renkančios informaciją tikslinės rinkodaros tikslais, tikėtina, bus labiau suinteresuotos analizuoti naujausius duomenis.

Vadinasi, duomenų saugojimo trukmės apribojimo principu siekiama užtikrinti, kad asmens duomenys nebūtų saugomi beatodairiškai. Dirbtinio intelekto gebėjimas saugoti asmens duomenis vis spartėja, o sąnaudos – mažėja, todėl išlieka rizika, kad asmens duomenų tvarkymas, naudojant dirbtinį intelektą gali būti nesuderinamas su duomenų saugojimo trukmės apribojimo principu.

3.6. Vientisumo ir konfidencialumo principas

BDAR 5 straipsnio 1 dalies f punkte nustatyta, kad „asmens duomenys turi būti: tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo". Aktualias nuostatas įtvirtina ir tarptautiniai teisės šaltiniai: Europos Tarybos duomenų apsaugos konvencijos 7 straipsnis ir EBPO privatumo gairių 11 straipsnis, kurie nustato pareigą apsaugoti asmens duomenis tinkamomis priemonėmis.

BDAR 5 straipsnio 1 dalies f punkto formuluotė suponuoja, kad „vientisumo ir konfidencialumo" principas reiškia saugumo reikalavimą (Kuner *et al.*, 2020, p. 318). Atskirai, vientisumas ir konfidencialumas apibrėžia klasikinius asmens duomenų saugumo pažeidimo kriterijus. Konkrečiai, vientisumo pažeidimas reiškia asmens duomenų pakeitimą, o konfidencialumas – siejamas su asmens duomenų atskleidimu ar naudojimu be leidimo (29 straipsnio duomenų apsaugos darbo grupė, 2014, p. 4). Saugumo reikalavimu yra siekiama užtikrinti asmens duomenų saugumą ir užkardyti galimą duomenų apsaugos pažeidimą (Zaleskis, 2019, p. 131). Kitaip tariant, tai reiškia, kad duomenų valdytojas turi užtikrinti, kad surinkti duomenys būtų apsaugoti nuo bet kokio neleistino ar neteisėto tvarkymo ir nuo bet kokio atsitiktinio praradimo, sunaikinimo ar

sugadinimo (Understanding the 7 Principles of..., 2021). Saugumo reikalavimas yra detalizuojamas BDAR 32 straipsnyje, kuriame įtvirtinama duomenų valdytojo ir duomenų tvarkytojo pareiga įgyvendinti tinkamas technines ir organizacines duomenų apsaugos priemones, kad būtų užtikrintas duomenų tvarkymo saugumas. Tačiau minėtos pareigos įgyvendinimas priklauso nuo duomenų valdytojo ir duomenų tvarkytojo diskrecijos, t. y. minėti subjektai turi laisvę nuspręsti, kokias ir kaip su duomenų tvarkymu susijusias technologijas ir organizacines priemones taikyti (Zaleskis, 2019, p. 130). Be to, nėra įtvirtinto duomenų saugumo priemonių sąrašo, todėl pasirenkant jas sprendžiama atsižvelgiant į technines galimybes, sąnaudas, duomenų tvarkymo pobūdį (Zaleskis, 2019, p. 130).

29 straipsnio duomenų apsaugos darbo grupė yra nurodžiusi, kad siekis užtikrinti duomenų saugumą, pirmiausia yra siejamas su vadinamu „duomenų potvynio“ efektu, kuris reiškia, kad tvarkomų asmens duomenų kiekis vis didėja ir šiam reiškiniui yra palanki technologinė plėtra, kadangi vis daugiau duomenų tampa prienami, ir keliauja po visą pasaulį. Antra, nuolatos didėjant asmens duomenų kiekiui, didėja jų vertė ir ekonominiu požiūriu. Šiuo metu neretai asmens duomenys yra valiuta mainais už internetinį turinį (29 straipsnio duomenų apsaugos darbo grupė, 2010b, p. 4-5). Atitinkamai, minėtos priežastys suponuoja poreikį taikyti griežtas apsaugos priemones ir duomenų valdytojų pareigą įdiegti efektyvias priemones asmens duomenų apsaugai, ypač kai asmens duomenys yra tvarkomi dirbtinio intelekto sistemų. Vis dėlto, minėtos pareigos įgyvendinimas dirbtinio intelekto kontekste yra sudėtingas. Kaip pastebėjo Jungtinės Karalystės informacijos tarnyba, neretai yra neįmanoma išvardyti visų saugumo rizikų, kurios gali kilti tvarkant asmens duomens naudojant dirbtinį intelektą. Dirbtinio intelekto poveikis saugumo reikalavimams užtikrinti gali priklausyti nuo to, kaip technologija buvo kuriama ir diegiama; esamų rizikos valdymo gebėjimų; dirbtinio intelekto sistemos pobūdžio ir jos taikymo apimties (How should we assess security..., 2022). Todėl duomenų valdytojams išlieka plati, tačiau atsakinga diskrecija nuspręsti, kokias su duomenų tvarkymu susijusias technologijas ir organizacines priemones turėtų pasitelkti, kai asmens duomenys yra apdorojami naudojant dirbtinį intelektą. Ekonominio bendradarbiavimo ir plėtros organizacijos rekomendacijose dėl dirbtinio intelekto principų pabrėžiami du būdai, kurie turėtų užtikrinti saugumo reikalavimo įgyvendinimą, kai naudojamos dirbtinio intelekto sistemos. Visų pirma, nurodoma, kad dirbtinio intelekto sistemų veikimui turi būti taikomas atsekamumo metodas, kuris gali padėti analizuoti dirbtinio intelekto sistemos rezultatus, duomenų šaltinius ir jų saugojimą. Tokiu būdu atsekamumas gali padėti suprasti dirbtinio intelekto priimtus sprendimus ir užkardyti galimas klaidas ateityje. Antra,

siūlomas rizikos valdymo metodas, kuriuo skatinama diegti į dirbtinio intelekto sistemas skaidrumą, atskaitomybę ir saugumą užtikrinančias priemones. Rizikos valdymo metodas turėtų būti taikomas per visa dirbtinio intelekto gyvavimo laikotarpį, siekiant nustatyti ir sušvelninti galimą riziką, kuri gali neigiamai paveikti dirbtinio intelekto sprendimus (Robustness, security and safety (Principle 1.4), 2019). Atitinkamai, manytina, kad saugumo reikalavimas yra aktualus kuriant ir diegiant dirbtinio intelekto sistemą, todėl duomenų valdytojai, kurie pasitelkia dirbtinį intelektą asmens duomenų tvarkymui, turėtų nuolatos atlikti techninę priežiūrą, reguliariai peržiūrint ir bandant dirbtinio intelekto sistemą, siekiant nustatyti galimus su duomenų tvarkymu susijusius pažeidimus.

Saugumo reikalavimo kontekste, aktualus ir Dirbtinio intelekto akto reguliavimas, kuriame laikomasi rizika pagrįsto požiūrio, pagal kurį taikomi skirtingi saugumo reikalavimai skirtingoms dirbtinio intelekto sistemų rūšims. Konkrečiai, Dirbtinio intelekto akte yra nustatyti reikalavimai didelės rizikos dirbtinio intelekto sistemoms. Pagal Dirbtinio intelekto akto 6 straipsnį, didelės rizikos dirbtinio intelekto sistema yra ta sistema, kuri yra kuriama, diegiama ar naudojame vienoje iš Dirbtinio intelekto akto III priede išvardintų sričių (pvz., biometrinės tapatybės nustatyme, švietime, užimtume, išmokų išmokėjime, teisėsaugoje ir pan.). Remiantis Dirbtinio intelekto aiškinamuoju memorandumu, didelės rizikos dirbtinio intelekto sistemos Europos Sąjungoje yra leidžiamos tik jei jos atitinka privalomus reikalavimus ir yra atliktas *ex ante* atitikties vertinimą. Šiuo atveju, didelės rizikos dirbtinio intelekto sistemų tiekėjai ir įstatymo nustatytais atvejais naudotojai (pvz., jei jie dirbtinio intelekto sistemą pradeda naudoti savo vardu) (Dirbtinio intelekto akto 28 straipsnio 1 dalies a punktas) turi užtikrinti rizikos valdymo sistemą, duomenų valdymą, techninę dokumentaciją, registraciją ir pan. (Dirbtinio intelekto akto 9-12 straipsniai). Manytina, kad minėtini reikalavimai galėtų būti aktualūs ir duomenų valdytojams, siekiant įgyvendinti saugumo reikalavimą, ir užtikrinti tinkamą asmens duomenų tvarkymą pasitelkiant dirbtinį intelektą.

Apibendrinant, galima teigti, kad vientisumo ir konfidencialumo principu yra įgyvendinamas saugumo reikalavimas, kuriuo įtvirtinama duomenų valdytojo ir duomenų tvarkytojo pareiga užtikrinti asmens duomenų saugumą ir užkardyti galimus asmens duomenų pažeidimus. Pasitelkiant dirbtinį intelektą asmens duomenų tvarkymui neretai yra neįmanoma išvardinti visų galimų saugumo rizikų, todėl duomenų valdytojas ir duomenų tvarkytojas turi inovatyviai vertinti būtinas technines ir organizacines priemones asmens duomenų tvarkymo saugumui užtikrinti.

3.7. Atskaitomybės principas

Pagrindinių duomenų apsaugos principų sąrašas baigiamas nurodant, kad duomenų valdytojas yra atsakingas už visų duomenų apsaugos principų laikymąsi (Kuner *et al.*, 2020, p. 318). Panašias nuostatas įtvirtina ir Europos Tarybos duomenų apsaugos konvencijos 10 straipsnis, ir EBPO privatumo gairių 14 straipsnis, kurie nustato duomenų valdytojo atsakomybę už pagrindinių duomenų apsaugos principų laikymąsi ir pažeidimą. Europos Sąjungos lygiu, BDAR 2 straipsnyje nustatyta, kad duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi duomenų apsaugos teisės principų, ir turi sugebėti įrodyti, kad jų laikomasi.

Terminas „atskaitomybė“ duomenų apsaugos teisėje nėra naujas. Sąvoka „atskaitomybė“ vartojama kaip atsakomybė už atliktas pareigas (Kuner *et al.*, 2020, p. 319-320). Iš pradžių atskaitomybė duomenų apaugos teisėje buvo siejama su duomenų valdytojo atsakomybe už tai, kad būtų laikomasi duomenų apsaugos taisyklių. Vėliau atskaitomybės reikšmė išsivystė iki aktyvių duomenų valdytojo veiksmų, pagal kuriuos duomenų valdytojas turi būti pasirengęs įrodyti, kad duomenys tvarkomi laikantis duomenų apsaugos principų (Kuner *et al.*, 2020, p. 561). Atitinkamai, visų pirma, atskaitomybės principas yra siejamas duomenų valdytojo atsakomybe už bet kokį duomenų tvarkymą įgyvendinant asmens duomenų apsaugos principus ne teoriškomis, o praktiškomis, konkrečiomis ir efektyviomis priemonėmis (29 straipsnio duomenų apsaugos darbo grupė, 2010b, p. 9). Kaip ir įgyvendinant vientisumo ir konfidencialumo principą, priemonių sąrašas, kurias gali įgyvendinti duomenų valdytojas yra nebaigtinis. Priemonės gali apimti tiek vidaus procedūrų atlikimą prieš pradedant tvarkyti asmens duomenis, duomenų apsaugos politikos nustatymą, išankstinį poveikio duomenų apsaugai vertinimą (Zaleskis, 2019, p. 136), duomenų apsaugos pareigūno paskyrimą, asmens duomenis tvarkančių asmenų (pvz., programuotojų, žmogiškųjų išteklių atstovų) mokymą, vidaus ir išorės auditą (29 straipsnio duomenų apsaugos darbo grupė, 2010b, p. 12). Antra, duomenų valdytojai turi galėti įrodyti, kad laikosi duomenų apsaugos principų. Šiuo tikslu duomenų valdytojas turėtų įrodyti, kokį poveikį turi priemonės, kurių yra imtasi ir kodėl šios priemonės yra veiksmingos (Europos duomenų apsaugos valdyba, 2020b, p. 29) (pvz., asmens duomenis tvarkant sutikimo pagrindu, duomenų valdytojas turėtų galėti įrodyti, kad duomenų subjektas sutiko dėl duomenų tvarkymo) (Zaleskis, 2019, p. 137).

Norvegijos duomenų apsaugos tarnyba yra nurodžiusi, kad duomenų apsaugos principas, kuriuo grindžiamas visas dirbtinio intelekto kūrimas ir taikymas, yra atskaitomybė (Norwegian Data Protection Authority, 2017, p. 25). Toks teiginys pagrįstas

atsižvelgiant į dirbtinio intelekto duomenų tvarkymą, kuris yra paremtas didelių duomenų kiekių analize ir sąsajų darymu, todėl neretai dirbtinio intelekto priimamų sprendimų nėra lengva paaiškinto, o tai kelia esminių atskaitomybės klausimų (Declaration on Ethics and Data..., 2018, p. 2). Tai suponuoja, kad naudojant dirbtinį intelektą asmens duomenų tvarkymui, gali trūkti aiškumo dėl dirbtinio intelekto galutinių priimtų sprendimų (Information Commissioner's Office, 2017, p. 51). Kaip pastebėjo Jungtinės Karalystės informacijos tarnyba, duomenų valdytojui gali kilti sunkumų nustatant, ar dirbtinis intelektas atlieka iš tikrųjų tai, ko yra tikimasi, ar dirbtinio intelekto veiksmai nėra šališki, klaidingi, nepagrįsti (Information Commissioner's Office, 2017, p. 51). Praktiniu požiūriu duomenų valdytojai ne visada gali būti subjektai, turintys faktinę, ekonominę ar net praktinę galią duomenų tvarkymo operacijoms, kai asmens duomenys yra tvarkomi pasitelkus dirbtinį intelektą. Atitinkamai, kai dirbtinis intelektas priima sprendimus, darančius poveikį duomenų subjektui, kyla klausimų, kas yra atsakingas už šiuos sprendimus, kai dėl tvarkomų duomenų sudėtingumo ir kiekio, atsakingo subjekto nėra įmanoma nustatyti (Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 368). Tai aktualu, kai dirbtinio intelekto sistemos yra įsigyjamos iš pasaulinio rinkų tiekėjų. Tuo atveju, kai dirbtinis intelektas yra laikomas produktu, kyla teisinis neaiškumas tarp asmeninės atsakomybės, kuri reglamentuojama pagal BDAR, ir atsakomybės už gaminius, kuri yra nereglamentuojama (Europos Parlamentas, Europos civilinės teisės...., 2016 cituota Europos Sąjungos pagrindinių teisių agentūra *et al.*, 2018, p. 362). Be to, Europos Sąjungos Parlamentas yra pažymėjęs, kad nors techniniu požiūriu tiesiogine arba netiesiogine žalos ar nuostolių priežastimi gali būti bet kuri dirbtinio intelekto sistemomis grindžiama fizinė ar virtuali veikla, prietaisai ar procesai, beveik visais atvejais jie yra sistemų kūrėjų, diegėjų arba jomis manipuliuojančių asmenų veiklos rezultatas. Laikosi nuomonės, kad dėl dirbtinio intelekto sistemų neaiškumo ir savarankiškumo praktiškai gali būti labai sunku ar netgi neįmanoma susieti konkrečių dirbtinio intelekto sistemų veiklos klaidų ir konkretaus asmens veiksmų, todėl šią kliūtį galima apeiti pareikalaujant įvairių asmenų, kurie kuria, prižiūrėti ir kontroliuoja su dirbtinio intelekto sistema susijusią riziką, atsakomybės (Europos Parlamento rezoliucija su rekomendacijomis Komisijai dėl..., 2020). Vis dėlto, šiuo atveju, BDAR jokių išimčių duomenų valdytojams nedaro. Priešingai, duomenų valdytojai turi pareigą imtis visų techninių ir organizacinių priemonių, kad užtikrintų, jog šie minėti dirbtinio intelekto tiekėjai teiktų BDAR atitinkančius produktus (BDAR 78 konstatuojamoji dalis).

Minėta, kad priemonių sąrašas, kurias gali įgyvendinti duomenų valdytojas, siekdama užtikrinti atskaitomybės principo laikymąsi, yra nebaigtinis. Specialiojoje

literatūroje pastebima, kad dirbtiniam intelektui tvarkant asmens duomenis yra itin aktualus poveikio duomenų apsaugai vertinimas, kuris gali padėti reaguojant į nenumatytus technologijų iššūkius, siekiant nustatyti rizikas ir jas sumažinti (Mitrou, 2019, p. 61-62). Poveikio duomenų apsaugai vertinimas yra aktualus, kai asmens duomenų tvarkymui naudojamos naujos technologijos ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą, tikslus, gali kilti didelis pavojų fizinių asmenų teisėms bei laisvėms (BDAR 35 straipsnio 1 dalis). Europos Sąjungos 29 straipsnio darbo grupė gairėse yra nurodyta, kad nuoroda į duomenų subjektų „teises bei laisves“ visų pirma yra susijusi su teisėmis į duomenų apsaugą, tačiau taip pat gali apimti ir kitas pagrindines teises, pavyzdžiui, žodžio, mintis ar judėjimo laisvę (29 straipsnio duomenų apsaugos darbo grupė, 2017c, p. 7). Tačiau BDAR nėra nustatyta, kaip turėtų būti aiškinamas „didelis pavojus“. BDAR 76 konstatuojamoje dalyje detalizuojama, kad pavojus turėtų būti vertinamas remiantis objektyviu įvertinimu. Atitinkamai, manytina, kad nepaisant „didelio pavojaus“ neapibrėžtumo, tikėtina, kad dauguma asmens duomenų, kurie yra tvarkomi pasitelkiant dirbtinį intelektą, turėtų patekti į poveikio duomenų apsaugai vertinimo kategoriją. Nekvestionuojama, kad dirbtinio intelekto taikymas susijęs su naujomis technologijomis, sudėtingais ir dažnai netikėtais sprendimais, paremtais asmens duomenų apdorojimu. Todėl siūloma, atsižvelgiant į dirbtinio intelekto prognozuojamąjį pobūdį ir į tai, kad iš anksto neretai yra sudėtinga apibrėžti konkrečius duomenų tvarkymo tikslus, privalomai atlikti poveikio duomenų apsaugai vertinimą kiekvieną kartą, kai yra naudojamas dirbtinis intelektas asmens duomenų tvarkymui (Schwartz, 2016). Vis dėlto, iššūkis, su kuriuo gali susidurti poveikio duomenų apsaugai vertinimas, kai siekiama tvarkyti asmens duomenis pasitelkiant dirbtinį intelektą yra tas, kad prognozavimas gali būti netikslus. Neretai vertinimai yra atliekami remiantis žinomais arba galimais technologijų taikymais. Be to, svarbus laiko faktorius, kuris suponuoja, kad nuo technologijos atsiradimo iki jos pasekmių suvokimo gali praeiti daug laiko, todėl atliktas išankstinis vertinimas gali būti neteisingas.

Apibendrinant tai, kas išdėstyta, galima teigti, kad atskaitomybės principu yra siekiama skatinti duomenų valdytojus priimti konkrečias, praktines priemones, kurios užtikrintų asmens duomenų principų įgyvendinimą ir gavus prašymą, įrodyti, kad ėmėsi šių priemonių užtikrinimo. Duomenų valdytojas, kuris naudoja dirbtinį intelektą, gali susidurti su atskaitomybės principo įgyvendinimo problematika, nes duomenų valdytojas ne visada gali būti asmuo turintis faktinę, ekonominę, praktinę galią kontroliuoti dirbtiniu intelektu pagrįstą asmens duomenų tvarkymą. Dėl šios problematikos kyla teisinis neaiškumas, kas turėtų būti atsakingas už dirbtinio intelekto priimtus sprendimus.

IŠVADOS

1. Dinamiška skaitmeninių technologijų pažanga lemia, kad nėra visuotinai pripažintos dirbtinio intelekto sampratos. Dirbtinio intelekto apibrėžimo kūrimas yra nuolatinis procesas, kuriuo turi būti atsižvelgiama į dirbtinio intelekto kontekstą ir pokyčius šioje srityje. Europos Sąjunga siekdama reglamentuoti dirbtinį intelektą, pateikė pasiūlymą dėl dirbtinio intelekto apibrėžties Dirbtinio intelekto akte ir suteikė Europos Sąjungos Komisijai įgaliojimus priimti deleguotuosius aktus, kuriais dirbtinio intelekto apibrėžimas būtų keičiamas atsižvelgiant į dirbtinio intelekto sistemų ir prietaisų pažangą. Šiuo metu dirbtinis intelektas yra neatsiejamas be mašininio ir giliojo mokymosi, kurių pagrindu dirbtinis intelektas yra grindžiamas asmens duomenų apdorojimu.

2. Dirbtinis intelektas yra neatsiejamas nuo asmens duomenų, nes kuriant ir naudojant dirbtinį intelektą yra tvarkomi asmens duomenys. Tai lemia, kad naudojant dirbtinį intelektą yra būtina užtikrinti Europos Sąjungos pagrindines teises, įskaitant teisę į duomenų apsaugą. Teisės į duomenų apsaugą užtikrinimas dirbtinio intelekto kontekste kelia iššūkių susijusių su dirbtinio intelekto tvarkomais neobjektyviais duomenimis, renkamu dideliu duomenų kiekiu ar neaiškių sprendimų priėmimu, dėl kurių fiziniai asmenys neretai negali tinkamai susipažinti su surinktais duomenis, juos kontroliuoti ar reikalauti, kad duomenys toliau nebūtų tvarkomi.

3. BDAR yra pagrindinė teisinė priemonė, kuri nustato duomenų apsaugos teisės normas, taikytinas dirbtiniam intelektui, nes dirbtinis intelektas yra neatsiejamas nuo automatizuotų sprendimų priėmimo tvarkant asmens duomenis. BDAR nenustato specialių taisyklių dirbtiniam intelektui, išskyrus BDAR 22 straipsnį. BDAR principai yra pagrindas visam BDAR rėžimui ir su jų taikymo problematika susiduria dirbtinis intelektas. Europos Sąjunga siekdama lyderystės dirbtinio intelekto srityje, inicijuoja teisės aktų pasiūlymus dirbtinio intelekto teisinio reglamentavimo srityje. Reikšmingas pasiūlymas dėl Dirbtinio intelekto akto, kuriuo siekiama užtikrinti teisėtą ir saugų dirbtinio intelekto naudojimą, tačiau Dirbtinio intelekto aktas susilaukė kritikos dėl teisinio aiškumo trūkumo, nes su duomenų tvarkymu susijusios teisės normos nepateikia jokių nuorodų į duomenų subjektų teises.

4. Asmens duomenų sąvoka aiškinama plačiai, o dirbtinio intelekto renkama informacija nėra atribota, todėl dirbtinis intelektas renka didelius kiekius duomenų apie fizinį asmenį

(duomenų subjektą) iš įvairių šaltinių: jutiklių, stebėjimo prietaisų, įrašų, susijusių su asmenų savybėmis ar elgsena. BDAR į dirbtinį intelektą, kaip duomenų valdytoją, nereferuojama ir laikomasi požiūrio, kad dirbtinio intelekto atliekamus procesus privalo koordinuoti asmuo, todėl iš duomenų apsaugos teisės kylančias pareigas privalo užtikrinti duomenų valdytojas, kuris priima sprendimus dėl dirbtinio intelekto tikslų ir priemonių. Duomenų tvarkytojas tvarko asmens duomenis duomenų valdytojo vardu ir nenaudoja asmens duomenų savo tikslams, todėl už BDAR pareigų įgyvendinimą yra atsakingas ribota apimtimi. Pagal teritorinio taikymo apimtį, dažniausiai dirbtinio intelekto naudotojai turi buveinę Europos Sąjungoje arba duomenų subjektas yra Europos Sąjungoje, ar duomenų valdytojo veikla yra susijęs su prekių ar paslaugų, arba duomenų subjektų elgesio stebėsena, todėl yra įpareigoti asmens duomenis tvarkyti pagal BDAR.

5. Teisėtumo principas yra neatsiejamas nuo teisėtų asmens duomenų tvarkymo pagrindų, kurių užtikrinimas dirbtinio intelekto kontekste kelia iššūkių, susijusių su neapibrėžtumu, kokiu išsamumu turėtų būti pagrįsti teisėti duomenų tvarkymo pagrindai, kai dirbtinis intelektas asmens duomenis tvarko dideliu mastu iš įvairių objektų teikiančių informaciją. Sąžiningumo principo įgyvendinamas siejamas su duomenų subjekto savarankiškumu, teisėtais lūkesčiai ir kvalifikuoto asmens įsikišimu tvarkant asmens duomenis, tačiau šio principo užtikrinimas naudojant dirbtinį intelektą susiduria su iššūkiais, nes duomenų subjektai nėra tinkamai informuojami, kada ir kokia apimtimi yra naudojamas dirbtinis intelektas, be to, egzistuoja galimas dirbtinio intelekto šališkumas, priklausantis nuo dirbtinio intelekto kūrimo ir naudojimo, todėl yra svarbu, kad duomenų valdytojai pasitelktų kvalifikuotus subjektus, kurie galėtų užtikrinti teisėtą duomenų tvarkymą. Skaidrumo principu užtikrinamas duomenų subjektų informavimas apie duomenų tvarkymą, tačiau didelį duomenų kiekį generuojanti, savaime besimokanti, su „juodosios dėžės“ problematika susijusi dirbtinio intelekto prigimtis, neužtikrina galimybės duomenų subjektams suteikti aiškią informaciją apie duomenų tvarkymą.

6. Duomenų tvarkymo tikslo apribojimo principu nustatoma, kad duomenų tvarkymo tikslas turi būti konkretus, aiškus ir teisėtas, ir tolimesnis duomenų tvarkymas turi būti suderintas su pirminiais duomenų tvarkymo tikslais. Dirbtinio intelekto kontekste, duomenų tvarkymo tikslo apribojimo principas nėra užtikrinamas, nes neretai dirbtinio intelekto sistemos duomenų tvarkymo tikslą apibrėžia itin plačiai, o dirbtinis intelektas yra grindžiamas savarankišku vystymusi, neapibrėžtais tikslais. Reikalavimas užtikrinti tolimesnį asmens duomenų tvarkymą suderintą su pirminiais susiduria su iššūkiais, nes

dirbtinis intelektas yra pagrįstas duomenų rinkimo paskirties keitimu ir geba asmens duomenis naudoti kitiems tikslams nei jie iš pradžių buvo surinkti. Su duomenų tvarkymo tikslo apribojimo principu susijęs duomenų kiekio mažinimo principas, nes aiškiai neapibrėžus konkrečių ir teisėtų duomenų tvarkymo tikslų yra neįmanoma užtikrinti, kad duomenys bus susiję su tikslais, neperteklinai, tinkami ir adekvatūs. Tai lemia, kad duomenų kiekio mažinimo principo įgyvendinimas prieštarauja dirbtinio intelekto sampratai, nes dirbtinis intelektas yra neatsiejamas nuo „duomenų maksimizavimo“ ir didžiųjų duomenų, kurie renka didelės apimties asmens duomenų kiekius iš įvairių šaltinių.

7. Duomenų tikslumo principas yra siejamas su reikalavimu užtikrinti, kad asmens duomenys būtų tikslūs ir prireikus atnaujinami. Duomenų tikslumo principas taikomas tiek objektyviai informacijai, tiek prognozėms, kurios dirbtinio intelekto kontekste gali būti netikslios tiek dėl duomenų, sugadintų techninio gedimo, tiek ir dėl žmogiškojo faktoriaus, kylančios dėl šališkų duomenų įvesčių. Dirbtinis intelektas gali toleruoti tam tikrą netikslių duomenų kiekį, kuris gali neturėti įtakos bendrųjų tendencijų nustatymui, tačiau tai neatleidžia duomenų valdytojų nuo pareigos užtikrinti duomenų tikslumą, kurį įgyvendinti yra sudėtinga dėl dirbtinio intelekto savybės rinkti ir tvarkyti didelius kiekius informacijos.

8. Vientisumo ir konfidencialumo principas reiškia saugumo reikalavimą, kuriuo siekiama užtikrinti asmens duomenų saugumą ir išvengti duomenų apsaugos pažeidimų. Dirbtinio intelekto kontekste saugumo reikalavimas neužtikrinamas visa apimtimi, nes nėra įmanoma išvardyti visų galimų saugumo rizikų, galinčių kilti tvarkant asmens duomenis dirbtinio intelekto sistema. Tai lemia, kad dirbtinio intelekto, kuris tvarko asmens duomenis, saugumas priklauso nuo technologijos kūrimo ir diegimo, esamų rizikos valdymo sistemų efektyvumo, dirbtinio intelekto sistemos pobūdžio ir taikymo apimties. Saugumo reikalavimui užtikrinti duomenų valdytojas turi plačią diskreciją nuspręsti, kokias technologijas ir organizacines priemones turi pasitelkti. Rekomenduojama naudoti atsekamumo ar rizikos valdymo metodus, siekiant užtikrinti skaidrumą, analizuoti dirbtinio intelekto priimtus sprendimus ir duomenų šaltinius visą dirbtinio intelekto gyvavimo laikotarpį.

ŠALTINIŲ SĄRAŠAS

Teisės norminiai aktai

Tarptautinės sutartys

1. Tarptautinio Teisingumo Teismo statutas (1946). *Valstybės žinios*, 2002, 15-557.
2. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis (1981). *Valstybės žinios*, 2001, 32-1059.

Europos Sąjungos teisės norminiai aktai

3. Europos Sąjungos sutartis (2008). *Europos Sąjungos oficialusis leidinys*, C 115/13.
4. Sutarties dėl Europos Sąjungos veikimo (2012). *Europos Sąjungos oficialusis leidinys*, C 326/47.
5. Europos Sąjungos pagrindinių teisių chartija (2016). *Europos Sąjungos oficialusis leidinys*, C 202/389.
6. Europos Parlamento ir Tarybos 2016 m. balandžio 27 d. reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). *OJ L 119*, p. 1
7. Europos Parlamento ir Tarybos 2021 m. balandžio 29 d. reglamentas (ES) 2021/694 kuriuo nustatoma Skaitmeninės Europos programa ir panaikinamas Sprendimas (ES) 2015/2240. *L 166/1*, p. 1

Lietuvos teisės norminiai aktai

8. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas (2018). TAR, 11733.

Soft law šaltiniai

9. Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais (2019a). DI apibrėžtis. Pagrindiniai pajėgumai ir mokslo šakos [interaktyvus]. Prieiga per internetą:

https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf [žiūrėta 2023 d. vasario 9 d.].
10. Aukšto lygio ekspertų grupė dirbtinio intelekto klausimais (2019b). Patikimo DI etikos gairės [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_LT.pdf [žiūrėta 2023 d. vasario 11 d.].
11. Europos 2023 m. sauso 23 d. deklaracija dėl skaitmeninio dešimtmečio skaitmeninių teisių ir principų. *2023/C 23/01*, p.1.
12. Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) gairės dėl privatumo apsaugos ir tarptautinių asmens duomenų srautų (1980). *OECD Legal Instruments*, 1980, OECD/LEGAL/0188.
13. Europos duomenų apsaugos priežiūros pareigūnas (2020). Opinion 4/2020 EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European approach to excellence and trust [interaktyvu]. Prieiga per internetą: https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf [žiūrėta 2023 m. vasario 25 d.].
14. Europos duomenų apsaugos valdyba (2019). Gairės Nr. 3/2018 dėl Bendrojo duomenų apsaugos reglamento teritorinės taikymo srities (3 straipsnis) [interaktyvu]. Prieiga per internetą: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_lt [žiūrėta 2023 m. vasario 11 d.].
15. Europos duomenų apsaugos valdyba (2021). Gairės Nr. 07/2020 dėl sąvokų „duomenų valdytojas" ir „duomenų tvarkytojas" pagal BDAR [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_lt [žiūrėta 2023 m. vasario 26 d.].
16. Europos duomenų apsaugos valdyba ir Europos duomenų apsaugos priežiūros pareigūnas (2021). Bendra nuomonė Nr. 5/2021 dėl pasiūlymo dėl Europos Parlamento ir Tarybos reglamento, kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio intelekto aktas) [interaktyvu]. Prieiga per internetą: https://edpb.europa.eu/system/files/2021-10/edpb-edps_joint_opinion_ai_regulation_lt.pdf [žiūrėta 2023 m. kovo 1 d.].
17. Europos Komisijos 2018 m. balandžio 25 d. Komunikatas Dirbtinis intelektas Europai. *COM(2018) 237 final*, p. 1.
18. Europos Komisijos 2019 balandžio 8 d. komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Pasitikėjimo į žmogų orientuotu dirbtiniu intelektu didinimas. *COM(2019) 168 final*, p. 1.

19. Europos Komisija (2020). Baltoji knyga. Dirbtinis intelektas. Europos požiūris į kompetenciją ir pasitikėjimą. Prieiga per internetą: https://op.europa.eu/lt/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1 [žiūrėta 2023 m. vasario 11 d.].
20. Europos Parlamento 2019 m. vasario 12 d. rezoliucija dėl visapusiškos Europos pramonės politikos dirbtinio intelekto ir robotikos srityje. *P8_TA(2019)0081*.
21. Europos Parlamento 2020 m. spalio 20 d. rezoliucija su rekomendacijomis Komisijai dėl dirbtinio intelekto, robotikos ir susijusių technologijų etinių aspektų sistemos. *P9_TA(2020)0275*.
22. Europos Parlamento 2021 m. gegužės 20 d. rezoliucija „Europos skaitmeninės ateities kūrimas: kliūčių bendrosios skaitmeninės rinkos veikimui šalinimas ir dirbtinio intelekto naudojimo gerinimas siekiant naudos vartotojams Europos Sąjungoje“ (2020/2216(INI)). *P9_TA(2021)0261*, p. 204.
23. European Parliamentary Research Service (2020). The impact of the General Data Protection Regulation (GDPR) on artificial intelligence [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/641530/EPRS_STU(2020)641530_EN.pdf [žiūrėta 2023 m. vasario 23 d.].
24. Europos ekonomikos ir socialinių reikalų komiteto 2022 m. lapkričio 22 d. nuomonė „Skaitmeninė tapatybė, duomenų suverenumas ir informacinėje visuomenėje gyvenantiems piliečiams skirtos teisingos skaitmeninės pertvarkos kelias“. *C 443/22*.
25. Europos regionų komiteto 2022 m. vasario 28 d. nuomonė „Europos požiūris į dirbtinį intelektą. Dirbtinio intelekto aktas“ (pataisyta nuomonė). *2022/C 97/12*, p. 60.
26. Specialusis dirbtinio intelekto skaitmeniniame amžiuje komitetas (2022). Pranešimas dėl dirbtinio intelekto skaitmeniniame amžiuje [interaktyvus]. Prieiga per internetą: https://www.europarl.europa.eu/doceo/document/A-9-2022-0088_LT.html [žiūrėta 2023 m. sausio 21 d.].
27. Europos Sąjungos pagrindinių teisių agentūra ir Europos Taryba (2018). Europos duomenų apsaugos teisės vadovas [interaktyvus]. Liuksemburgas: Europos Sąjungos leidinių biuras. Prieiga per internetą: https://op.europa.eu/lt/publication-detail/-/publication/af9d0b3f-82be-11e5-b8b7-01aa75ed71a1 [žiūrėta 2023 m. vasario 1 d.].
28. Europos Vadovų Tarybos 2017 m. spalio 19 d. susitikimo išvados. *EUCO 14/17*.
29. 29 straipsnio duomenų apsaugos darbo grupė (2007). Nuomonė 4/2007 dėl asmens duomenų sąvokos [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2007/wp136_lt.pdf [žiūrėta 2023 m. vasario 1 d.].
30. 29 straipsnio duomenų apsaugos darbo grupė (2010a). Nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf [žiūrėta 2023 m. vasario 26 d.].
31. 29 straipsnio duomenų apsaugos darbo grupė (2010b). Opinion 3/2010 on the principle of accountability [interktyvus]. Prieiga per internetą: https://www.dataprotection.ro/servlet/ViewDocument?id=720 [žiūrėta 2023 m. vasario 1 d.].
32. 29 straipsnio duomenų apsaugos darbo grupė (2011). Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_lt.pdf [žiūrėta 2023 m. vasario 23 d.].
33. 29 straipsnio duomenų apsaugos darbo grupė (2013). Nuomonė Nr. 03/2013 dėl tikslo ribojimo [interaktyvus]. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/wp203_en.pdf [žiūrėta 2023 m. vasario 20 d.].
34. 29 straipsnio duomenų apsaugos darbo grupė (2014). Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf [žiūrėta 2023 m. vasario 13 d.].
35. 29 straipsnio duomenų apsaugos darbo grupė (2017a). Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės [interaktyvus]. Prieiga per internetą: https://www.teismai.lt/data/public/uploads/2020/02/20180411_skaidrumo_uztikrinimo_gaires.pdf [žiūrėta 2023 m. vasario 20 d.].
36. 29 straipsnio duomenų apsaugos darbo grupė (2017b). Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės [interaktyvus]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/items/612053/en [žiūrėta 2023 m. kovo 23 d.].
37. 29 straipsnio duomenų apsaugos darbo grupė (2017c). Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų [interaktyvus]. Prieiga

per internetą: https://am.lrv.lt/uploads/am/documents/files/wp248_PDAV_gaires_2017-04-04.pdf [žiūrėta 2023 m. sausio 28 d.].
38. Europos duomenų apsaugos valdyba (2020b). Gairės 4/2019 dėl 25 straipsnio. Pritaikytoji ir standartizuotoji duomenų apsauga [interaktyvus]. Prieiga per internetą: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_lt.pdf [žiūrėta 2023 m. kovo 1 d.].

Specialioji literatūra

39. Albrecht, J. P. (2016). Regaining Control and Sovereignty in the Digital Age. Iš: Wright, D. ir Hert, D. P. (2016). *Enforcing Privacy. Regulatory, Legal and Technological Approaches*. Switzerland: Springer.
40. Bathaee, Y. (2018). The artificial intelligence black box and the failure of intent and causation. Iš: *Volume 31, Number 2 Spring 2018*. United States: Harvard Journal of Law & Technology.
41. Crawford, K., Whittaker, M. (2016). *The Social and Economic Implications of Artificial Intelligence Technologies in the Near-Term*. United States: New York University's Information Law Institute.
42. Dogarua, L. (2020). *The Main Goals of the Fourth Industrial Revolution. Renewable Energy Perspectives.* Romania: Procedia Manufacturing 46 (2020) 397–401.
43. Kuner, C., Bygrave, L. A. ir Docksey, C. (red.) (2020). *The EU General Data Protection Regulation (GDPR) A Commentary*. United Kingdom: Oxford University Press.
44. Kuner, C., Bygrave, L. A. ir Docksey, C. (red). (2021). *The EU General Data Protection Regulation: A Commentary. Update of Selected Articles*. United Kingdom: Oxford University Press.
45. Marengo, F. (2021). *Data Protection Law in Charts. A Visual Guide to the General Data Protection Regulation*. Varese.
46. Mitrou, L. (2019). *Data protection, artificial intelligence and cognitive sertives. Is the General Data Protection Regulation (GDPR) "Artificial intelligence-proff"?* Greece: University of Economics and Business - Department of Informatics.
47. Paal., B. (2022). *Artificial Intelligence as a Challenge for Data Protection Law And Vice Versa. Responsible Data Governance.* United Kingdom: Cambridge University Press.
48. Purtova, N. (2018). The law of everything. Broad concept of personal data and future of EU data protection law. Netherlands: Routledge.

49. Russell, S., Norvig, P. (2016). *Artificial intelligence. A Modern Approach. Third Edition*. New Jersey: PearsonEducation,Inc.
50. Wallace, N., Castro, D. (2018). *The Impact of the EU's New Data Protection Regulation on AI*. United States: Center for Data Innovation.
51. Zaleskis, J. (2019). *Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Monografija. Vilnius: VĮ Registrų centras.

Elektroniniai leidiniai

52. Agencia Española Protección Datos (2020). GDPR compliance of processings that embed Artificial Intelligence An introduction [interaktyvus]. Prieiga per internetą: https://www.aepd.es/es/documento/adecuacion-rgpd-ia-en.pdf [žiūrėta 2023 m. sausio 19 d.].
53. Berryhill, J., Berryhill, J., Heang, K. K., Clogher, R., McBride, K. (2019). Hello, World: Artificial intelligence and its use in the public sector [interaktyvus]. OECD Working Papers on Public Governance. Prieiga per internetą: https://www.ospi.es/export/sites/ospi/documents/documentos/Tecnologias-habilitantes/IA-Public-Sector.pdf [žiūrėta 2023 m. sausio 21 d.].
54. Botelho, B., Bigelow, S. J. (2023). What is Big Data and Why it is Important? [interaktyvu]. Prieiga per internetą: https://www.techtarget.com/searchdatamanagement/definition/big-data [žiūrėta 2023 m. vasario 1 d.]
55. BasuMallick, C. (2022). What Is Big Data? Definition, Types, Importance, and Best Practices [interaktyvu]. Prieiga per internetą: https://www.spiceworks.com/tech/big-data/articles/what-is-big-data/ (žiūrėta 2023 m. vasario 3 d.).
56. Butterworth, M. (2018). The ICO and artificial intelligence: The role of fairness in the GDPR framework [interaktyvus]. Prieiga per internetą: https://www.sciencedirect.com/science/article/abs/pii/S026736491830044X [žiūrėta 2023 m. vasario 1 d.].
57. Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data (2019). Artificial Intelligence and Data Protection: Challenges and Possible Remedies [interaktyvus]. Prieiga per internetą: https://rm.coe.int/artificial-intelligence-and-data-protection-challenges-and-possible-re/168091f8a6 [žiūrėta 2023 m. vasario 18 d.].

58. Centre for Information Policy Leadership (2018). Artificial Intelligence and Data Protection: Delivering Sustainable AI Accountability in Practice. First Report: Artificial Intelligence and Data Protection in Tension [interaktyvus]. Prieiga per internetą: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_first_ai_report_-_ai_and_data_protection_in_tension__2_.pdf [žiūrėta 2023 m. sausio 20 d.].

59. Downey, L., Anderson, S. ir Kvilhaug, S. (2022). What an Algorithm Is and Implications for Trading [interaktyvus]. Prieiga per internetą: https://www.investopedia.com/terms/a/algorithm.asp [žiūrėta 2023 m. vasario 7 d.].

60. Drake, M., Ong. J., Hansen, M. ir Peets, J. (2023). EU AI Policy and Regulation: What to look out for in 2023 [interaktyvus]. Prieiga per internetą: https://www.insideprivacy.com/artificial-intelligence/eu-ai-policy-and-regulation-what-to-look-out-for-in-2023/ [žiūrėta 2023 m. vasario 10 d.].

61. Europarl.europa.eu. *Artificial Intelligence ante portas: Legal & ethical reflections*. Prieiga per internetą: https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf [žiūrėta 2023 m. vasario 27 d.].

62. Entrepreneur. *ChatGPT: What Is It and How Does It Work?* (modifikuota 2018-02-16). Prieiga per internetą: https://www.entrepreneur.com/science-technology/chatgpt-what-is-it-and-how-does-it-work/445014 [žiūrėta 2023 m. kovo 8 d.].

63. Eimin.Lrv. *Lietuvos dirbtinio intelekto strategija. Ateities vizija* [interaktyvus]. Prieiga per internetą: https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf [žiūrėta 2023 m. vasario 6 d.].

64. Europarl.europa.eu. *Artificial Intelligence ante portas: Legal & ethical reflections*. Prieiga per internetą: https://www.europarl.europa.eu/at-your-service/files/be-heard/religious-and-non-confessional-dialogue/events/en-20190319-artificial-intelligence-ante-portas.pdf [žiūrėta 2023 m. vasario 27 d.].

65. En-gb.Facebook. Privacy Policy. What is the Privacy Policy and what does it cover? (modifikuota 2023-01-01). Prieiga per internetą: https://en-gb.facebook.com/privacy/policy/?entry_point=data_policy_redirect&entry=0 [žiūrėta 2023 m. kovo 1 d].

66. GDPRHub. *Commentary*. Prieiga per internetą: https://gdprhub.eu/Article_5_GDPR#Commentary [žiūrėti 2023 m. vasario 18 d.].

67. Heilweil, R. (2020). AI is finally good at stuff, and that's a problem [interaktyvus]. Prieiga per internetą: https://www.vox.com/recode/2022/12/7/23498694/ai-artificial-intelligence-chat-gpt-openai [žiūrėta 2023 m. kovo 2 d.].

68. Hamon, R., Junklewitz, H. ir Sanchez, I. (2020). Robustness and Explainability of Artificial Intelligence [interaktyvus]. European Commission. Prieiga per internetą: https://publications.jrc.ec.europa.eu/repository/handle/JRC119336 [žiūrėta 2023 m. vasario 3 d.].

69. ICO.org. *How should we assess security and data minimisation in AI?* Prieiga per internetą: https://ico.org.uk/for-organisations/guide-to-data-protection/key-dp-themes/guidance-on-ai-and-data-protection/how-should-we-assess-security-and-data-minimisation-in-ai/ [žiūrėta 2023 m. sausio 25 d.].

70. Information Commissioner's Office (2017). Big data, artificial intelligence, machine learning and data protection [interaktyvus]. Prieiga per internetą: https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf [žiūrėta 2023 m. vasario 3 d.].

71. International Conference of Data Protection & Privacy Commissioners (2018). Declaration on ethics and data protection in artifical intelligence [interaktyvus]. Prieiga per internetą: http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf [žiūrėta 2023 m. sausio 19 d.].

72. International Working Group on Data Protection in Telecommunications (2018). Working Paper on Privacy and Artificial Intelligence [interaktyvus]. Prieiga per internetą: https://www.bfdi.bund.de/SharedDocs/Downloads/EN/Berlin-Group/20181130_WP_Artificial-Intelligence.pdf?__blob=publicationFile&v=1 [žiūrėta 2023 m. vasario 2 d.].

73. Intellias. *How to Train and AI with DGPR Limitations* (modifikuota 2022-01-13). Prieiga per internetą: https://intellias.com/how-to-train-an-ai-with-gdpr-limitations/ [žiūrėta 2023 m. kovo 3 d.].

74. Kanade, V. (2022). What Is Artificial Intelligence (AI)? Definition, Types, Goals, Challenges, and Trends in 2022 [interaktyvus]. Prieiga per internetą: https://www.spiceworks.com/tech/artificial-intelligence/articles/what-is-ai/ [žiūrėta 2023 m. vasario 23 d.].

75. Leong, B. ir R. Jordan, S. (2020). The Spectrum of Artificial Intelligence. Companion to the FPF AI Infographic [interaktyvus]. The Future of Privacy Forum. Prieiga internete: https://fpf.org/wp-content/uploads/2021/08/FPF-AIEcosystem-Report-FINAL-Digital.pdf [žiūrėta 2023 m. sausio 21 d.].

76. Mach. *This basketball-playing robot is so good it could outshoot Stephen Curry* [interaktyvus] (modifikuota 2018-03-20). Prieiga per internetą:

https://www.nbcnews.com/mach/science/basketball-playing-robot-so-good-it-could-outshoot-stephen-curry-ncna858011 [žiūrėta 2023 m. vasario 1 d.].

77. Mathworks. *What Is Machine Learning? How it works, why it matters, and getting started* [interaktyvus]. Prieiga per internetą: https://www.mathworks.com/discovery/machine-learning.html [žiūrėta 2023 d. vasario 2 d.].

78. Norwegian Data Protection Authority (2018). Artificial intelligence and privacy [interaktyvus]. The Norwegian Data Protection Authority. Prieiga per internetą: https://www.datatilsynet.no/globalassets/global/english/ai-and-privacy.pdf [žiūrėta 2023 m. sausio 22 d.].

79. OECD.AI. Robustness, security and safety (Principle 1.4). Prieiga per internetą: https://oecd.ai/en/dashboards/ai-principles/P8 [žiūrėta 2023 m. vasario 11 d.].

80. Onetrust. Understanding the 7 Principles of the GDPR (modifikuota 2021-05-17). Prieiga per internetą: https://www.onetrust.com/blog/gdpr-principles/#Integrity [žiūrėta 2023 m. kovo 3 d.].

81. Policies. Google. *Why Google collects data* (modifikuota 2022-12-15). Prieiga per internetą: https://policies.google.com/privacy?fg=1#whycollect [žiūrėta 2023 m. kovo 1 d.].

82. Room document for the 38th International Conference of Data Protection and Privacy Commissioners (2016). Artificial Intelligence, Robotics, Privacy and Data protection [interaktyvu]. Prieiga per internetą: https://edps.europa.eu/sites/default/files/publication/16-10-19_marrakesh_ai_paper_en.pdf [žiūrėta 2023 m. vasario 3 d.].

83. Roach, J. (2018). Microsoft improves facial recognition technology to perform well across all skin tones, genders [interaktyvus]. Prieiga per internetą: https://blogs.microsoft.com/ai/gender-skin-tone-facial-recognition-improvement/ [žiūrėta 2023 m. sausio 25 d.].

84. Richards, N. M, Jonathan H. K. (2013). Three Paradoxes of Big Data [interaktyvus]. Prieiga per internetą: https://www.stanfordlawreview.org/online/privacy-and-big-data-three-paradoxes-of-big-data/ [žiūrėta 2023 m. vasario 1 d.].

85. Simplilearn. *Netflix Recommendations: How Netflix Uses AI, Data Science, And ML*. Prieiga per internetą: https://www.simplilearn.com/how-netflix-uses-ai-data-science-and-ml-article [žiūrėta 2023 m. vasario 8 d.].

86. Schwartz, P. (2016). Risk and high risk: Walking the GDPR tightrope [interaktyvus]. Prieiga per internetą: https://iapp.org/news/a/risk-and-high-risk-walking-the-gdpr-tightrope/ [žiūrėta 2023 m. sausio 19 d.].
87. Study Requested by the ITRE committee (2020). Opportunities of Artificial Intelligence [interaktyvu]. Prieiga per internetą: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652713/IPOL_STU(2020)652713_EN.pdf [žiūrėta 2023 m. vasario 7 d.].
88. TheEconomicTimes. *What is algorithm? Definition of Algorithm, Algorithm meaning* [interaktyvus]. Prieiga per internetą: https://economictimes.indiatimes.com/definition/algorithm [žiūrėta 2023 m. vasario 7 d.].
89. Uwex.wisconsin.edu. *What Is Big Data?* (modifikuota 2015-05-18). Prieiga per internetą: https://uwex.wisconsin.edu/stories-news/what-is-big-data/ (žiūrėta 2023 m. vasario 3 d.).
90. Vale, B. S. (2022). GDPR and the AI Act interplay: lessons from FPF's adm case-law report [interaktyus]. Prieiga per internetą: https://fpf.org/blog/gdpr-and-the-ai-act-interplay-lessons-from-fpfs-adm-case-law-report/ [žiūrėta 2023 m. vasario 23 d.].
91. Victor Demiaux, V. ir Si Abdallah, Y. (2017). How can humans keep the upper hand? The ethical matters raised by algorithms and artificial intelligence [interaktyvus]. French data aprotection authorty. Prieiga per internetą: https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_ai_gb_web.pdf [žiūrėta 2023 m. sausio 23 d.].
92. Visier. *What the GDPR Shows Us About the Future of AI Regulation*. Prieiga per internetą: https://www.visier.com/blog/what-the-gdpr-shows-us-about-the-future-of-ai-regulation/ [žiūrėta 2023 m. sausio 27 d.].
93. Zannoni, L. ir Propato, M. (2022). AI and GDPR: A tight affair [interaktyvu]. Prieiga per internetą: https://www.dentons.com/en/insights/articles/2022/april/20/ai-and-gdpr-a-tight-affair [žiūrėta 2023 m. vasario 8 d.].
94. Ziyad, M. (2018/2019). Artificial Intelligence Definition, Ethics and Standards [interaktyvu]. Prieiga per internetą: https://www.researchgate.net/publication/332548325_Artificial_Intelligence_Definition_Ethics_and_Standards [žiūrėta 2023 m. vasario 3 d.].

Teismų praktika

Europos Sąjungos Teisingumo Teismo praktika

95. *Lauermann* [ESTT], Nr. C-139/01, [2003-04-20]. ECLI:EU:C:2003:294.
96. *Lindqvist* [ESTT], Nr. C-101/01, [2003-11-06]. ECLI:EU:C:2003:596.
97. *Volker und Markus Schecke ir Eifert* [ESTT], Nr. C-92/09, [2010-11-09]. ECLI:EU:C:2010:662.
98. *Schwarz* [ESTT], Nr. C-291/12 [2013-10-17]. ECLI:EU:C:2013:670.
99. *Digital Rights Ireland ir Seitlinger ir kt.* [ESTT], Nr. C-293/12 [2014-04-08]. ECLI:EU:C:2014:238.
100. *Google Spain ir Google* [ESTT], Nr. C-131/12, [2014-05-13]. ECLI:EU:C:2014:317.
101. *YS ir kt.* [ESTT], Nr. C-141/12, [2014-07-17]. ECLI:EU:C:2014:2081.
102. *Ryneš* [ESTT], Nr. C-212/13 [2014-12-11]. ECLI:EU:C:2014:2428
103. *Breyer* [ESTT], Nr. C-582/14, [2016-10-19]. ECLI:EU:C:2016:779.
104. *Tele2 Sverige* [ESTT], Nr. C-203/15, [2016-12-21]. ECLI:EU:C:2016:970.
105. *Rīgas satiksme* [ESTT], Nr. C-13/16, [2017-05-04]. ECLI:EU:C:2017:336.
106. *Nowak* [ESTT], Nr. C-434/16, [2017-12-20]. ECLI:EU:C:2017:994.
107. *Asociaţia de Proprietari bloc M5A-ScaraA* [ESTT], Nr. C-708/18, [2019-12-11]. ECLI:EU:C:2019:1064.
108. *Land Hessen* [ESTT], Nr. C-272/19, [2020-07-09]. ECLI:EU:C:2020:535.
109. *Orange Romania* [ESTT], Nr. C-61/19, [2020-11-11]. ECLI:EU:C:2020:901.

Lietuvos teismų praktika

110. Lietuvos vyriausiojo administracinio teismo 2012 m. liepos 26 d. sprendimas administracinėje byloje Nr. A858-2133/2012.
111. Lietuvos vyriausiojo administracinio teismo 2012 m. gruodžio 18 d. sprendimas administracinėje byloje Nr. A143-2740-12.
112. Vilniaus apygardos administracinio teismo 2020 m. gegužės 28 d. sprendimas administracinėje byloje Nr. EI2-3383-473/2020.

Kiti šaltiniai

Travaux préparatoires

113. Europos Komisijos 2021 m. balandžio 21 d. pasiūlymas Europos Parlamento ir Tarybos reglamentas kuriuo nustatomos suderintos dirbtinio intelekto taisyklės (Dirbtinio

intelekto aktas) ir iš dalies keičiami tam tikri Sąjungos teisėkūros procedūra priimti aktai. *COM(2021) 206 final*, p. 1.

SANTRAUKA

ES Bendrojo duomenų apsaugos reglamento principų problematika dirbtinio intelekto kontekste

Domantė Mozerytė

Sparčiai vystantis skaitmeninėms technologijoms, kiekvienais metais sugeneruojama vis daugiau duomenų. Technologinė pažanga yra neatsiejama nuo dirbtinio intelekto vystymosi, kuris kelia iššūkių, susijusių su teise į asmens duomenų apsaugą. Dėl asmens duomenų tvarkymo dirbtiniam intelektui yra taikomas BDAR, kuriuo nustatomi duomenų apsaugos standartai, įskaitant BDAR principus. BDAR (išskyrus BDAR 22 straipsnį) nepateikia konkrečių nuostatų, kaip reikėtų užtikrinti duomenų apsaugos normų įgyvendinimą dirbtiniam intelektui. Atitinkamai, pasitelkiant dirbtinį intelektą asmens duomenų tvarkymui, svarbu atsižvelgti į BDAR principus, kurie yra pagrindas viso BDAR rėžimo ir su kurių taikymo iššūkiais susiduria dirbtinis intelektas.

Pirmojoje darbo dalyje analizuojama dirbtinio intelekto samprata, iššūkiai, susiję su duomenų apsaugos teise ir dirbtinio intelekto reguliavimo sritis duomenų apsaugos kontekste. Atskleidžiama problematika susijusi su dirbtinio intelekto apibrėžtimi. Analizuojama teisė į duomenų apsaugą dirbtinio intelekto kontekste ir nagrinėjami dirbtiniam intelektui aktualūs teisės šaltiniai. BDAR principai yra neatsiejami nuo bendrųjų BDAR nuostatų, todėl antrojoje darbo dalyje yra atskleidžiama asmens duomenų, duomenų subjekto sampratos, duomenų valdytojo ir duomenų tvarkymo santykis su dirbtiniu intelektu ir BDAR teritorinė taikymo sritis dirbtinio intelekto kontekste. Trečiojoje dalyje analizuojami BDAR 5 straipsnyje įtvirtinti principai, jų samprata ir su jų taikymu susijusi problematika, kai asmens duomenys yra tvarkomi pasitelkiant dirbtinį intelektą.

SUMMARY

Issue of the Principles of the EU General Data Protection Regulation in the Context of Artificial Intelligence

Domantė Mozerytė

With the dynamic development of digital technologies, more and more data is being generated every year. Technological progress is inseparable from the development of artificial intelligence, which raises challenges in the context of the right to protection of personal data. The processing of personal data by artificial intelligence is subject to the GDPR, which sets out data protection standards, including the GDPR principles. The GDPR (with the exception of Article 22 of the GDPR) does not contain specific provisions on how data protection standards should be enforced in relation to artificial intelligence. Therefore, when using artificial intelligence to process personal data, it is essential to take into account the principles of the GDPR, which are the basis for the whole GDPR regime and whose application challenges artificial intelligence faces.

The first part of the thesis analyses the concept of artificial intelligence, the challenges related to data protection law and the scope of regulation of artificial intelligence in the context of data protection. The issues related to the definition of artificial intelligence are identified. Analyses the right to data protection in the context of artificial intelligence and examines the sources of law relevant to artificial intelligence. The principles of the GDPR are inseparable from the general provisions of the GDPR, and the second part of the work therefore highlights the concepts of personal data, the data subject, the relationship between the data controller and data processing in relation to artificial intelligence, and the territorial scope of the GDPR in the context of artificial intelligence. The third part analyses the principles enshrined in Article 5 of the GDPR, their conception and the issues related to their application when personal data are processed by means of artificial intelligence.