Vilniaus universiteto Teisės fakulteto

Viešosios teisės katedra

Aistės Kabašinskaitės,
V kurso, Tarptautinės ir Europos Sąjungos teisės
studijų šakos studentės

Magistro darbas

ES Bendrojo duomenų apsaugos reglamento vaidmuo ketvirtojoje pramonės revoliucijoje

Vadovas: lekt. dr. Julius Zaleskis

Recenzentė: lekt. dr. Erika Leonaitė

Vilnius

2020

TURINYS

SĄVOKŲ SĄRAŠAS 3
ĮVADAS 4
1. ASMENS DUOMENŲ APSAUGOS TEISĖ IR TECHNOLOGIJŲ RAIDA 9
1.1. Asmens duomenų apsaugos teisės samprata ir turinys 9
1.1.1. Asmens duomenų sąvoka 9
1.1.2. Specialiųjų kategorijų asmens duomenys 12
1.2. Asmens duomenų apsaugos teisės principai 13
1.3. Asmens duomenų apsaugos teisės ir technologijų raidos tarpusavio ryšys 19
2. ES BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS KAIP KETVIRTOSIOS PRAMONĖS REVOLIUCIJOS TECHNOLOGIJŲ REGULIAVIMO ŠALTINIS 28
2.1. ES Bendrojo duomenų apsaugos reglamento reikšmė ir pagrindiniai tikslai 28
2.2. Asmens duomenų apsaugos naujovės ES Bendrajame duomenų apsaugos reglamente 31
2.3. Teritorinė ES Bendrojo duomenų apsaugos reglamento taikymo sritis 36
2.4. Duomenų subjektų teisės bei jų įgyvendinimas 41
3.ES BENDROJO DUOMENŲ APSAUGOS REGLAMENTO ĮTAKA KETVIRTOSIOS PRAMONĖS REVOLIUCIJOS TECHNOLOGIJŲ PLĖTRAI 47
3.1. Bendrasis duomenų apsaugos reglamentas ir didieji duomenys 48
3.2. Bendrasis duomenų apsaugos reglamentas ir dirbtinis intelektas 53
3.3. Bendrasis duomenų apsaugos reglamentas ir daiktų internetas 56
3.4. Bendrasis duomenų apsaugos reglamentas ir „Blockchain“ technologija 60
3.5. ES Bendrojo duomenų apsaugos reglamento taikymo iššūkiai ir ateities perspektyvos ketvirtojoje pramonės revoliucijoje 64
IŠVADOS 69
LITERATŪROS BEI KITŲ ŠALTINIŲ SĄRAŠAS 72
SANTRAUKA 80
SUMMARY 81

SĄVOKŲ SĄRAŠAS

Asmens duomenys	bet kuri informacija, susijusi su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta arba gali būti nustatyta (Bendrojo duomenų apsaugos reglamento 4 str. 1 d.)
Duomenų subjektas	fizinis asmuo, kurio asmeniniai duomenys yra renkami, laikomi ir tvarkomi (Bendrojo duomenų apsaugos reglamento 4 str. 1 d.)
Duomenų valdytojas	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kitas organas, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus, sąlygas ir būdus tvarkomi (Bendrojo duomenų apsaugos reglamento 4 str. 7 d.)
Duomenų tvarkytojas	fizinis arba juridinis asmuo, valdžios institucija, agentūra ar bet kuris kitas organas, kuris duomenų valdytojo pavedimu tvarko asmens duomenis (Bendrojo duomenų apsaugos reglamento 4 str. 8 d.)
Duomenų tvarkymas	bet kuri operacija ar operacijų rinkinys, automatiniais arba neautomatiniais būdais atliekamus su asmens duomenimis, kaip antai: rinkimas, užrašymas, rūšiavimas, saugojimas, adaptavimas ar keitimas, atgaminimas, paieška, naudojimas, atskleidimas perduodant, platinant ar kitu būdu padarant juos prieinamus, išdėstymas reikiama tvarka ar sujungimas derinant, blokavimas, trynimas ar naikinimas tvarkomi (Bendrojo duomenų apsaugos reglamento 4 str. 2 d.)

ĮVADAS

Pastarųjų metų technologijų bei mokslo pažanga lėmė didelius pokyčius mūsų gyvenime. Ženkliai padidėjo asmens duomenų rinkimo bei tvarkymo mastai. Informacinių technologijų dėka atsirado naujų būdų kaip rinkti bei tvarkyti asmens duomenis precedento neturinčiais kiekiais. Mokslininkai daug kalba apie ketvirtosios pramonės revoliucijos pradžią, prie kurios kūrimo prisidės visos šalys, o jos teikiamas galimybės žmonija pajus daugelyje sričių.[1] Sparčiai tobulėjant informacinėms technologijoms bei plečiantis skaitmeninei rinkai, iškilo naujų pavojų, susijusių su asmens duomenų apsauga. Dėl šios priežasties, stipriai sumažėjo pasitikėjimas tuometiniu asmens duomenų apsaugos teisiniu reguliavimu, kurio pagrindas buvo 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Duomenų apsaugos direktyva). Atsirado būtinybė suvienodinti ir sugriežtinti teisinį reguliavimą bei išplėsti duomenų subjektų teises asmens duomenų apsaugos srityje, todėl 2016 m. balandžio 27 d. Europos Sąjunga priėmė Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (toliau - Bendrasis duomenų apsaugos reglamentas). Šis teisės aktas iš esmės keičia duomenų apsaugos reglamentavimą visoje Europos Sąjungoje. Atsižvelgus į tai, šiame darbe analizuojamas Bendrasis duomenų apsaugos reglamentas ir jo naujovės, nagrinėjamas asmens duomenų apsaugos teisės ir naujųjų technologijų sąryšis, taip pat Bendrojo duomenų apsaugos reglamento reikšmė bei įtaka ketvirtosios pramonės revoliucijos technologijoms.

Temos aktualumas. Šis darbas yra aktualus tuo, jog jame analizuojamas visiškai naujas ekonomikos raidos etapas, pasižymintis skaitmeninių technologijų pažanga, lemiančia

[1] SCHWAB, Klaus. The Fourth Industrial Revolution. *World Economic Forum*, 2016, p. 8.

reikšmingus pokyčius ekonomikos, pramonės, verslo, medicinos, socialinio gyvenimo bei kitose srityse. Svarbu pabrėžti, jog ketvirtoji pramonės revoliucija išsiskiria savo greičiu bei plėtra. Kiekvieną dieną pasaulyje sukuriama maždaug 2,5 kvintilijonų baitų duomenų, o tai reiškia, kad apie 90 proc. pasaulyje egzistuojančių duomenų sugeneruota vos per kelis pastaruosius metus. Prognozuojama, kad 2020 m. prie interneto bus prijungta 50 mlrd. įrenginių (2015 m. buvo 10 mlrd.)[2]. Sparčiai didėjant duomenų tvarkymo mastams, kyla daugelis klausimų dėl tolimesnio asmens duomenų apsaugos užtikrinimo naujųjų technologijų amžiuje, todėl jaučiamas didelis teisininkų bei kitų sričių specialistų susidomėjimas šia tema. Šiame darbe analizuojamas Bendrojo duomenų apsaugos reglamentas, kuris yra pagrindinis duomenų apsaugos teisės šaltinis Europos Sąjungoje, jo reikšmė bei įtaka tolimesnei mokslo ir technologijų pažangos raidai. Didelis dėmesys skiriamas asmens duomenų apsaugos teisės bei naujųjų technologijų sąryšiui atskleisti. Taip pat nagrinėjami Bendrojo duomenų apsaugos reglamento taikymo iššūkiai ir ateities perspektyvos ketvirtojoje pramonės revoliucijoje, kuri neišvengiamai palies kiekvieną iš mūsų. Atsižvelgus į tai, darbas aktualus tiek teoriškai, tiek praktiškai.

Darbo originalumas. Teisės doktrinoje Bendrojo duomenų apsaugos reglamento bei ketvirtosios pramonės revoliucijos santykis nagrinėtas itin mažai. Lietuvoje šią temą plačiau nagrinėjo tik Julius Zaleskis[3]. Tuo tarpu, užsienio autoriai analizavo Bendrojo duomenų apsaugos reglamento įtaką tik pavienėms ketvirtosios pramonės revoliucijos technologijoms, nedarydami sisteminės analizės. Michael Butterworth[4] nagrinėjo Bendrojo duomenų apsaugos

[2] World Economic forum. Survey Report. *Global Agenda Council on the Future of Software & Society Deep Shift Technology Tipping Points and Societal Impact*, 2015 [interaktyvus, žiūrėta 2020 m. kovo 30 d.]. Prieiga per internetą: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.
[3] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 317-325.
[4] BUTTERWORTH, Michael. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2018, p. 1-2.

reglamento įtaką dirbtiniam intelektui, Lachlan Urquhart bei kiti[5] tyrė Bendrajame duomenų apsaugos reglamente įtvirtintos atskaitomybės pareigos įgyvendinimo problematiką daiktų internetui. Tal Zarsky[6] analizavo Bendrojo duomenų apsaugos reglamento suderinamumą su technologijomis, naudojančiomis didžiuosius duomenis, o Christopher Kuner[7] nagrinėjo „Blockchain“ technologijos santykį su Bendruoju duomenų apsaugos reglamentu. Atsižvelgus į tai, šis darbas išsiskiria tuo, jog atskleidžia Bendrojo duomenų apsaugos reglamento reikšmę bei įtaką ketvirtosios pramonės revoliucijai, analizuodamas naująsias technologijas tiek atskirai, tiek bendrame kontekste.

Tyrimo objektas. Šiame darbe analizuojamas Bendrasis duomenų apsaugos reglamentas bei jo vaidmuo ketvirtojoje pramonės revoliucijoje.

Darbo tikslas. Atskleisti Bendrojo duomenų apsaugos reglamento reikšmę bei įtaką naujųjų technologijų pažangai ir nustatyti jo santykį su ketvirtąja pramonės revoliucija.

Uždaviniai:

1) išnagrinėti asmens duomenų apsaugos teisės sampratą bei turinį;
2) atskleisti asmens duomenų apsaugos teisės ir technologijų raidos tarpusavio ryšį;
3) aptarti pagrindines Bendrojo duomenų apsaugos reglamento naujoves bei jų įgyvendinimo ypatumus;
4) išnagrinėti Bendrojo duomenų apsaugos reglamento taikymo problematiką, susijusią su ketvirtosios pramonės revoliucijos technologijų: didžiųjų duomenų analizės, dirbtinio intelekto, daiktų interneto bei „blockchain“ technologijos naudojimu praktikoje;

[5] URQUHANT Lachlan; LODGE, Tom; CRABTREE, Andy. Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, 2019, 27, p. 1–27.
[6] ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 [interaktyvus, žiūrėta 2020-03-05]. Prieiga per internetą: https://ssrn.com/abstract=3022646.
[7]KUNER, Christopher; CATE, Fred; LYNSKEY, Orla; , MILLARD, Christopher; LOIDEAIN, Ni Nora, SVANTESSON, Dan. Blockchain versus data protection. *International Data Privacy Law*, Volume 8, Issue 2, May 2018, p. 103–104 [interaktyvus]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipy009.

5) atskleisti Bendrojo duomenų apsaugos reglamento reikšmę bei įtaką ketvirtosios pramonės revoliucijos technologijų pažangai.

Tyrimo metodai. Šiame darbe naudojami toliau nurodyti tyrimų metodai:

1) **Lingvistinis:** Šis metodas padėjo išanalizuoti pagrindines sąvokas: duomenų subjektas, duomenų valdytojas, ketvirtoji pramonės revoliucija, didieji duomenys, dirbtinis intelektas ir t.t. bei kitus, su šiomis sąvokomis susijusius, apibrėžimus.
2) **Sisteminis:** Šis metodas buvo naudojamas detaliai nagrinėjant Bendrojo duomenų apsaugos reglamento bei kitų šiame darbe minėtų teisės aktų nuostatas kaip sistemą, išskiriant svarbiausius šių nuostatų aspektus ir pateikiant apibendrinančias išvadas.
3) **Lyginamasis**. Naudojant šį metodą, buvo lyginami skirtingi mokslo bei technologijų raidos etapai, taip pat lyginami buvęs duomenų apsaugos teisinis reguliavimas, įtvirtintas Duomenų apsaugos direktyvoje su naujuoju teisiniu reguliavimu, įtvirtintu Bendrajame duomenų apsaugos reglamente.
4) **Kritinės analizės**. Šis metodas buvo naudojamas analizuojant Bendrojo duomenų apsaugos reglamento ypatumus, jų naudą bei galimus įgyvendinimo iššūkius ketvirtojoje pramonės revoliucijoje.

Svarbiausi šaltiniai. Pagrindiniai šio darbo tyrimo šaltiniai buvo Bendrasis duomenų apsaugos reglamentas bei kiti tarptautiniai ir Europos Sąjungos norminiai teisės aktai, kuriuose įtvirtintos pagrindinės asmens duomenų apsaugos nuostatos ir principai – Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, Europos Sąjungos pagrindinių teisių chartija bei 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Nr. 108. Teorinei medžiagai buvo naudojami asmens duomenų apsaugos teisės vadovėliai, monografijos, užsienio bei Lietuvos teisės mokslininkų darbai, tarp kurių: Juliaus

Zaleskio[8], Ilonos Petraitytės[9], Mindaugo Civilkos[10], Christopher Kuner[11], Orla Lindskey[12], Peter Carey[13], Klaus Schwab[14] ir kt. darbai. Šiame darbe, taip pat, buvo naudojamasi reikšmingais *soft law* šaltiniais, tarp kurių Europos duomenų apsaugos valdybos gairės, Europos Sąjungos 29 straipsnio duomenų apsaugos darbo grupės nuomonės bei Europos Komisijos komunikatai. Papildomai buvo remiamasi ir aktualia Europos Sąjungos Teisingumo Teismo praktika.

[8] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019.
[9] PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174.
[10] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015 t. 96, p. 128-143.
[11]KUNER, Christopher. European Data Protection Law. Corporate Regulation and Compliance. *Oxford University Press*, 2nd edition, 2007.
[12] LINDSKEY, Orla. The Foundations of EU Data Protection Law. *Oxford University Press*, 2015.
[13] CAREY, Peter. Data Protection - A Practical Guide to UK and EU Law. *Oxford University Press*, 5th Edition, 2018.
[14] SCHWAB, Klaus. The Fourth Industrial Revolution. *World Economic Forum*, 2016.

1. ASMENS DUOMENŲ APSAUGOS TEISĖ IR TECHNOLOGIJŲ RAIDA

1.1. Asmens duomenų apsaugos teisės samprata ir turinys

Asmens duomenų apsaugos teisę nagrinėjantys mokslininkai pateikia gana panašią asmens duomenų apsaugos sąvoką. Pasak Lee A. Bygrave, asmens duomenų apsauga – tai priemonių (teisinių ir/ar neteisinių), skirtų apsaugoti asmenis nuo žalos, kurią sukelia informacijos apie juos tvarkymas (automatiniu ir/ar rankiniu būdu) ir apimančių tam tikrus principus, išdėstytus pripažįstamuose dokumentuose, rinkinys[15]. Teisės mokslininkas Frits W. Hondius asmens duomenų apsaugą supranta kaip teisių, laisvių ir esminių interesų apsaugą tvarkant su asmenimis susijusią informaciją, ypač kai informacijos tvarkymo procesuose padeda kompiuteriai[16]. Tuo tarpu, Europos Sąjungos teisė išskiria teisę į asmens duomenų apsaugą kaip vieną pagrindinių žmogaus teisių šiandieniniame pasaulyje. Europos Sąjungos pagrindinių teisių chartijos 8 straipsnyje numatyta, jog "kiekvienas turi teisę į savo asmens duomenų apsaugą". Atkreiptinas dėmesys, jog vienas iš svarbiausių Bendrojo duomenų apsaugos reglamento tikslų yra apsaugoti fizinių asmenų pagrindines teises ir laisves, o visų pirma jų teisę į asmens duomenų apsaugą. Europos Tarybos 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Nr. 108 (toliau – Konvencija Nr. 108) duomenų apsaugą apibrėžia kaip „visumą apsaugos priemonių, kurios neleistų asmens duomenų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti". Tačiau, siekiant iki galo suprasti asmens duomenų apsaugos teisę bei jos pagrindinius tikslus, pirmiausia būtina atlikti asmens duomenų sąvokos analizę.

1.1.1. Asmens duomenų sąvoka

[15] BYGRAVE, A. Lee. Data Privacy Law: An International Perspective. *Oxford University Press; 1 edition.* 2014, 25 p.
[16] HONDIUS, W. Frits. Emerging data Protection in Europe, *Amsterdam, North Holland Publishing Company*. 1975, 32 p.

Bendrajame duomenų apsaugos reglamente nurodyta, jog „asmens duomenys - tai bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių - vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius“[17]. Atitinkamai, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme[18] yra pateikiama analogiška asmens duomenų sąvoka – „tai bet kuri informacija, susijusi su fiziniu asmeniu (duomenų subjektu), kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai“. Atsižvelgus į tai, galime išskirti keturis svarbiausius aspektus, apibūdinančius, kokie duomenys yra laikytini asmens duomenimis.

Pirma, tai „bet kokia informacija“. Tai reiškia, jog ši informacija gali būti išreiškiama bei saugoma bet kokia forma. Ji apima vaizdo, garso, skaitmeninius, tekstinius, biometrinius duomenis, DNR duomenis ir t.t. Tokia informacija gali būti pateikiama raidėmis, skaičiais, grafiniu vaizdu, garsu ir kitomis formomis: pvz.: rašytinė informacija, kompiuterio bei kitų išmaniųjų įrenginių atmintyje saugoma skaitmeninė informacija, stebėjimo kamerų vaizdo įrašai ir t.t. Svarbu pabrėžti, kad asmens duomenimis galima laikyti ir informaciją, esančią laisvai pateiktame elektroninio dokumento tekste, jeigu ji atitinka kitus asmens duomenų

[17] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4, p. 1-88.
[18] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, Nr. 63-1479

apibrėžties kriterijus. Pavyzdžiui, elektroniniame laiške gali būti asmens duomenų[19]. Taigi, informacija apie asmenį gali būti tiek objektyvi, tiek ir subjektyvi, neatsižvelgiant į jos formą bei techninę laikmeną, kurioje ji yra pateikiama.

Antra, asmens duomenys yra „informacija susijusi su fiziniu asmeniu“. Kitaip tariant, tai tam tikra informacija apie fizinį asmenį. Duomenys laikomi susiję su asmeniu, jei jie nurodo asmens tapatybę, ypatybes ar elgesį arba jei tokia informacija naudojama siekiant nustatyti, kaip elgiamasi su tuo asmeniu arba kaip jis vertinamas, arba daryti susijusį poveikį[20].

Trečia, asmens duomenimis laikoma informacija susijusi su „fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta“. Į asmens duomenų sąvoką įeina visi duomenys, kurie identifikuoja ar padeda identifikuoti fizinį asmenį (kai fizinis asmuo yra išskiriamas iš visų kitų tai grupei priklausančių asmenų). Kaip jau minėta, tai gali būti tiek objektyvi, tiek ir subjektyvi informacija, svarbiausia, jog ji būtų susijusi su konkrečiu fiziniu asmeniu. Asmens duomenų apibrėžimas akcentuoja dviejų tipų informaciją – informaciją, pagal kurią asmens tapatybė gali būti nustatyta tiesiogiai (pvz.: vardas ir pavardė, asmens kodas, paso numeris ir t.t.) ir informaciją, pagal kurią asmens tapatybė gali būti nustatyta netiesiogiai, t. y. kai turimų duomenų nepakanka konkrečiam asmeniui nustatyti, tačiau kartu surinkta skirtinga informacija gali atskleisti konkretaus asmens tapatybę (pvz.: automobilio valstybinis numeris, telefono numeris, kraujo grupė, batų dydis, medicininės sveikatos istorija ir kt.). Tai teoriškai leidžia apimti labai daug duomenų, kurie *prima facie* turi labai menką ryšį su konkrečiu asmeniu. Todėl duomenys gali būti asmeniniai netgi jeigu jų pagalba fizinis asmuo gali būti identifikuotas tik kombinacijoje su kitais – pagalbiniais duomenimis[21].

[19]ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 4/2007 dėl asmens duomenų sąvokos*. 01248/07/LT WP 136, p. 7.
[20] 2005 m. sausio 19 d. darbo grupės dokumentas Nr. WP 105 „Darbo dokumentas dėl duomenų apsaugos klausimų, susijusių su RDA technologija“, p. 8.
[21] CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 130.

Ketvirta, ši informacija turi būti susijusi su „fiziniu asmeniu“. Čia galima išskirti du aspektus: informacija privalo būti susijusi su gyvu asmeniu ir tokia sąvoka gali būti taikoma tik fiziniams asmenims. Bendrasis duomenų apsaugos reglamentas nėra taikomas mirusiems asmenims, nes asmeniui mirus, jo teisės, asmens duomenų apsaugos atžvilgiu, pasibaigia. Nepaisant to, informacijai apie mirusius asmenis gali būti taikoma speciali apsauga, kurią užtikrina kiti norminiai teisės aktai, pvz.: Lietuvos Respublikos civilinis kodeksas[22], reglamentuojantis asmens teisę į savo atvaizdą ir ginantis asmens garbę bei orumą net ir po asmens mirties. Tuo tarpu, sąvoka „asmens duomenys“ gali būti taikoma tik fizinių asmenų duomenims, kadangi asmens duomenų apsaugos teisė nereglamentuoja juridinio asmens statusą turinčių subjektų duomenų[23].

1.1.2. Specialiųjų kategorijų asmens duomenys

Atkreiptinas dėmesys, kad Bendrojo duomenų apsaugo reglamente, taip pat, išskiriami ir specialių kategorijų asmens duomenys. Pabrėžtina, kad tai duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius, filosofinius įsitikinimus ar narystę profesinėse sąjungose, taip pat, genetiniai, biometriniai duomenys, padedantys konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenys, duomenys apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją bei asmens duomenys, susiję su apkaltinamaisiais nuosprendžiais ir nusikalstamomis veikomis[24]. Minėti duomenys laikomi specialiaisiais dėl jų ypač privataus pobūdžio, todėl jiems suteikiama ypatinga apsauga bei žymiai griežtesni teisiniai reikalavimai. Šiuo atžvilgiu, tvarkyti (rinkti bei naudoti) specialiųjų kategorijų asmens duomenis galima tik

[22] Lietuvos Respublikos civilinis kodeksas (su pakeitimais ir papildymais). *Valstybės žinios*, 2000-09-06, Nr. 74-2262.
[23] CAREY, Peter. Data Protection - A Practical Guide to UK and EU Law. *Oxford University Press*, 3rd Edition, 2009, p. 1
[24] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4, p. 1-88.

esant sąlygoms, nurodytoms Bendrajame duomenų apsaugos reglamente, pavyzdžiui: gavus aiškų duomenų subjekto sutikimą tokius duomenis tvarkyti arba jeigu asmens duomenis tvarkyti būtina dėl svarbių su viešuoju interesu susijusių priežasčių remiantis Europos Sąjungos arba nacionaline teise ir kt.[25] Visais kitais atvejais, specialių kategorijų asmens duomenis tvarkyti yra griežtai draudžiama. Toks pat draudimas galioja ir automatizuotam atskirų sprendimų priėmimui. Bendrojo duomenų apsaugos reglamento 22 straipsnio 4 dalis numato jog „draudžiama naudoti specialių kategorijų duomenis tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamų sprendimų priėmimui, dėl kurių duomenų subjektui gali kilti teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį“.

1.2. Asmens duomenų apsaugos teisės principai

Svarbų vaidmenį asmens duomenų apsaugos teisėje užima ir asmens duomenų apsaugos teisės principai, kuriais yra grindžiamas asmens duomenų apsaugos teisinis reglamentavimas ir be kurių negali būti sistemiškai aiškinamos bei tinkamai taikomos asmens duomenų tvarkymą reguliuojančios teisės normos[26]. Pagrindiniai šaltiniai, įtirtinantys asmens duomenų apsaugos principus, yra 1980 m. Ekonominio Bendradarbiavimo ir Plėtros Organizacijos (EBPO) Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių (toliau – Privatumo gairės), Konvencija Nr. 108, Duomenų apsaugos direktyva bei Bendrasis duomenų apsaugos reglamentas. Privatumo gairės yra laikomos fundamentaliu aktu, kadangi tai pirmasis tarptautinis dokumentas, susisteminęs bei įtvirtinęs pagrindinius asmens duomenų apsaugos principus. Kitaip tariant, Privatumo gairės buvo visuotinai pripažintos kaip tarptautiniu lygmeniu priimtinas ir technologiniu atžvilgiu

[25] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4, p. 1-88
[26] PETRAITYRĖ, Ilona. Asmens duomenų apsaugos teisiniai principai. Daktaro disertacija, 2013, p. 96.

neutralus privatumo apsaugos principų rinkinys[27]. Nors Privatumo gairės ir nebuvo teisiškai privalomos, tačiau stipriai įtakojo vėlesnį valstybių teisinį reglamentavimą asmens duomenų apsaugos srityje. Privatumo gairės suformulavo bei įtvirtino aštuonis bendruosius asmens duomenų apsaugos principus: asmens duomenų rinkimo apribojimo principą, asmens duomenų kokybės principą, tikslo nustatymo principą, asmens duomenų naudojimo apribojimo principą, asmens duomenų saugumo užtikrinimo principą, atvirumo principą, individualaus dalyvavimo principą bei atskaitomybės principą. Tuo tarpu Konvencija Nr. 108, Duomenų apsaugos direktyva ir Bendrasis duomenų apsaugos reglamentas šiuos principus patikslino bei išplėtė jų turinį.

Vienas pagrindinių asmens duomenų apsaugos principų yra teisėtumo, sąžiningumo ir skaidrumo principas. Pirmą kartą apie šį principą buvo užsiminta Privatumo gairėse, kurios numatė, jog asmens duomenys privalo būti renkami teisėtomis ir sąžiningomis priemonėmis ir, kai tinkama, su duomenų subjekto žinia arba sutikimu[28]. Vėliau, šis principas buvo paminėtas ir Konvencijoje Nr. 108, pagal kurią, tvarkomi asmens duomenys turi būti gauti ir tvarkomi sąžiningai ir teisėtai, saugomi konkrečiam bei teisėtam tikslui ir nenaudojami kitu šiam tikslui prieštaraujančiu būdu[29]. Kitaip nei minėtuose tarptautiniuose dokumentuose, Duomenų apsaugos direktyvoje buvo kalbama apie „teisingą ir teisėtą asmens duomenų tvarkymą“[30]. Tačiau, pirmą kartą oficialiai, teisėtumo, sąžiningumo ir skaidrumo principas buvo įtvirtintas Bendrajame duomenų apsaugos reglamente. Šio teisės akto 5 straipsnis numato, kad „asmens duomenys turi būti duomenų subjekto atžvilgiu tvarkomi teisėtu, sąžiningu ir skaidriu būdu.“

Pažymėtina, jog šis principas susideda iš trijų dalių: teisėtumo, sąžiningumo bei

[27] CIVILKA, M. Asmens duomenų apsaugos teisinis reguliavimas internet kontekste [interaktyvus], p. 9, [žiūrėta 2020 m. kovo 8 d.]. Prieiga per internetą: http://media.search.lt/GetFile.php?OID=92932&FID=269994
[28] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1999, Paris, p. 1
[29] 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Nr. 108, *Valstybės žinios*. 2001, Nr. 32-1059.
[30] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, Specialusis leidimas, OL L 281, p. 1-31.

skaidrumo. Teisėtumas reiškia, jog asmens duomenys turi būti tvarkomi laikantis teisės aktais nustatytų reikalavimų, t.y. asmens duomenys turėtų būti tvarkomi gavus atitinkamo duomenų subjekto sutikimą arba remiantis kitu teisiniu pagrindu, nustatytu Bendrajame duomenų apsaugos reglamente arba – kai šiame reglamente nurodoma – kitame Europos Sąjungos teisės akte ar Europos Sąjungos valstybės narės teisėje. Tuo tarpu, sąžiningumo principas įtvirtina bendro pobūdžio duomenų valdytojų ir duomenų tvarkytojų pareigą tvarkyti duomenis sąžiningai. Sąžiningumo standartai nulemia tai, kad duomenų subjekto sutikimas dėl duomenų tvarkymo neturėtų būti laikomas duotas laisva valia, jei duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti, nepatirdamas žalos (Bendrojo duomenų apsaugos reglamento preambulės 42 p.). Skaidrumo reikalavimas užtikrina, kad duomenų valdytojai ir duomenų tvarkytojai būtų atskaitingi duomenų subjektui bei padeda įgyvendinti duomenų subjektų galimybę kontroliuoti savo asmens duomenis. Skaidrumas, taip pat, yra susijęs su duomenų subjektų informavimu apie duomenų valdytojo tapatybę ir duomenų tvarkymo tikslus, taip pat su tolimesniu informavimu, kad būtų užtikrintas sąžiningas ir skaidrus duomenų tvarkymas atitinkamų fizinių asmenų atžvilgiu, jų teise gauti patvirtinimą dėl su jais susijusių asmens duomenų tvarkymo ir teise tuos duomenis gauti[31]. Svarbu pabrėžti, kad duomenų subjektai privalo būti informuoti apie jų teises, asmens duomenų tvarkymo apsaugos priemones, kurios bus naudojamos renkant bei tvarkant tokius duomenis bei kylančius pavojus, susijusius su asmens duomenų tvarkymu. Duomenų subjektai, taip pat, privalo būti informuoti ir apie tai, kaip naudotis savo teisėmis tokio asmens duomenų tvarkymo srityje. Ši informacija turi būti aiški, glausta ir skaidri bei pateikta lengvai prieinama forma.

Ne ką mažiau svarbus yra duomenų tvarkymo tikslo apribojimo principas. Šis principas reikalauja, kad asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais

[31] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės*. WP260, 1 red. 17/LT, p. 6.

tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu[32]. Atsižvelgus į tai, galima išskirti tris reikalavimus duomenų tvarkymo tikslams, kuriuos nulemia duomenų tvarkymo apribojimo principas: duomenų tvarkymo tikslai turi būti nustatyti iš anksto, jie turi būti aiškiai apibrėžti ir teisėti. Duomenų tvarkymo tikslo (ar tikslų) nurodymas yra asmens duomenų apsaugos teisinės sistemos pagrindas. Tai yra vienas iš esminių reikalavimų teisėto ir tinkamo asmens duomenų tvarkymo atžvilgiu. Asmens duomenų tvarkymo tikslai turi būti aiškiai atskleisti, paaiškinti ar išreikšti tam tikra suprantama forma.[33] Kitaip tariant, duomenų subjektui neturi kilti sunkumų šiuos tikslus suprasti. Tuo tarpu, teisėtumo reikalavimas reiškia, kad asmens duomenų tvarkymo tikslai turi „atitikti įstatymą“ plačiausia įmanoma prasme. Šis reikalavimas detalizuoja teisėtumo principą ir reikalauja individualaus situacijos vertinimo kiekvienu konkrečiu atveju. Kiekvienu atveju būtina įvertinti, kokioje srityje veikia duomenų valdytojas ir nustatyti jam taikomus teisės aktus, įskaitant civilinės, darbo, vartotojų teisių apsaugos, mokesčių teisės ir kitose srityse. Teisės prasme, nustatant, ar tam tikras tikslas yra teisėtas, taip pat, gali būti atsižvelgiama į kitus elementus, tokius kaip tam tikros šalies teisės papročiai, etikos kodeksas ir t.t., tačiau svarbu pabrėžti, jog tikro tikslo teisėtumas laikui bėgant gali keistis priklausomai nuo mokslo ir technologijų raidos bei visuomenės ir kultūrinių požiūrių pokyčių. Apibendrinant, darytina išvada, jog duomenų tvarkymo apribojimo principo tikslas yra apsaugoti duomenų subjektą, nustatant ribas duomenų valdytojams, kaip jie gali naudoti duomenų subjektų asmens duomenis ir užtikrinti tokio duomenų tvarkymo sąžiningumą.[34]

Svarbu paminėti ir asmens duomenų kiekio mažinimo principą, kuris reikalauja, kad asmens duomenys būtų adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie

[32] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.
[33] *Ibid*, 13 str. 4 d.
[34] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 03/2013 dėl tikslo apribojimo*, Nr. WP 203, 00569/13/LT, p. 12.

tvarkomi[35]. Pagal šį principą, asmens duomenų kiekis privalo būti ribojamas, pagal tai, kiek asmens duomenų yra būtina rinkti, atsižvelgiant į tikslus, kuriais šie duomenys yra tvarkomi. Taigi, duomenų valdytojas kiekvienu atveju privalo įvertinti kiek asmens duomenų reikia, norint pasiekti duomenų tvarkymo tikslus, bei užtikrinti, jog nebūtų renkami su šiais tikslais nesusiję asmens duomenys (t.y. asmens duomenys nebūtų pertekliniai). Pabrėžtina, kad šis principas yra glaudžiai susijęs su tikslo apribojimo principu.

Bendrajame duomenų apsaugos reglamente numatytas ir asmens duomenų tikslumo principas, kuris numato pareigą duomenų valdytojui imtis visų pagrįstų priemonių užtikrinti, kad duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi. Asmens duomenų tikslumą reikėtų suprasti kaip duomenų atitikimą faktinei tikrovei.[36] Atsižvelgus į tai, duomenų tikslumo principas būtų pažeistas jeigu duomenų valdytojas tvarkytų asmens duomenis žinodamas, kad jie yra netikslūs ar pasenę. Tuo tarpu, asmens duomenų saugojimo trukmės apribojimo principas įpareigoja duomenų valdytoją laikyti duomenų subjekto asmens duomenis tokia forma, kad duomenų subjekto tapatybę būtų galima nustatyti ne ilgesniam terminui nei būtina tais tikslais, kuriais asmens duomenys yra tvarkomi[37]. Pažymėtina, jog Bendrasis duomenų apsaugos reglamentas nenustato konkrečių asmens duomenų saugojimo terminų. Dėl šios priežasties, duomenų valdytojas privalo pats nusistatyti duomenų ištrynimo arba periodinės peržiūros terminus, kurie privalo būti ne ilgesni, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi (Bendrojo duomenų apsaugos reglamento preambulės 39 p.).

[35] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.
[36] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019
[37] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.

Bendrajame duomenų apsaugos reglamente teisės akte įtvirtintas vientisumo bei konfidencialumo principas, kitaip vadinamas duomenų saugumo principu, kuriuo dar labiau sustiprinama asmens duomenų apsauga. Šiuo atžvilgiu, konfidencialumas reiškia, kad duomenų tvarkymo sistemos ir paslaugos negali leisti atskleisti jokių asmens duomenų ar panaudoti jų be leidimo. Tuo tarpu, vientisumas reiškia, jog naudojamos technologijos turi užtikrinti, kad asmens duomenys nebūtų pakeisti[38]. Pagal šį principą, asmens duomenys privalo būti tvarkomi tokiu būdu ir taikant tokias technines bei organizacines priemones, jog būtų užtikrinamas pavojų atitinkančio lygio asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo[39]. Tokios priemonės galėtų apimti, *inter alia*, kuo mažesnės apimties asmens duomenų tvarkymą, kuo skubesnį pseudonimų suteikimą asmens duomenims ir t.t. Nepaisant šio reikalavimo, būtina atsižvelgti ir į duomenų valdytojo techninių priemonių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat, į tokio asmens duomenų tvarkymo keliamus pavojus fizinių asmenų teisėms ir laisvėms (Bendrojo duomenų apsaugos reglamento preambulės 78 p.).

Pabrėžtinas ir atskaitomybės principas, kuris yra išskirtinai svarbus duomenų valdytojams. Šis principas įtvirtina duomenų valdytojų pareigą įgyvendinti duomenų apsaugos principus ne teoriškai, o praktiškai, pasitelkiant tam tinkamas bei veiksmingas priemones. Šis principas reiškia duomenų valdytojo atsakomybę už bet kokį duomenų valdytojo arba jo vardu vykdomą asmens duomenų tvarkymą[40]. Dar daugiau, minėtas principas reikalauja, kad duomenų valdytojai prisiimtų atsakomybę už visų minėtų principų įgyvendinimą bei,

[38] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 03/2014 dėl pranešimo apie asmens duomenų saugumo pažeidimą*, Nr. WP 213 18/LTWP250, 1 red., p. 4.
[39] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.
[40] ES 29 str. duomenų apsaugos darbo grupė. *2010 m. Nuomonė 3/2010 dėl atskaitomybės principo*, Nr. WP173, p. 19.

pareikalavus, sugebėtų įrodyti, kad šių principų yra tinkamai laikomasi. Tuo pačiu, duomenų valdytojai yra atsakingi ir už priemones, kuriomis įgyvendinami asmens duomenų apsaugos teisės principai. Kaip vienas iš atskaitomybės principo įgyvendinimo pavyzdžių galėtų būti Bendrajame duomenų apsaugos reglamente numatyta duomenų valdytojo pareiga nedelsiant pranešti kompetentingai priežiūros institucijai apie duomenų saugumo pažeidimą, jei įmanoma, nuo to laiko, kai apie tai buvo sužinota, praėjus ne daugiau kaip 72 valandoms.

Atsižvelgus į tai, kas išdėstyta, darytina išvada, jog minėtais principais yra grindžiamas asmens duomenų apsaugos teisinis reguliavimas bei užtikrinamas tinkamas teisės aktų asmens duomenų apsaugos srityje įgyvendinimas.

1.3. Asmens duomenų apsaugos teisės ir technologijų raidos tarpusavio ryšys

Svarbu pabrėžti, asmens duomenų apsaugos teisė yra glaudžiai susijusi su mokslo bei technologijų raida. Tiesą sakant, viena iš pagrindinių priežasčių, lemiančių asmens duomenų apsaugos teisės koncepcijos susiformavimą bei tolimesnį šios teisės vystymąsi, buvo informacinių technologijų revoliucija, įvykusi XX a. antrojoje pusėje.[41] Atsižvelgus į tai, tikslinga aptarti asmens duomenų apsaugos teisės koncepcijos bei technologijų revoliucijos istorinę raidą.

Revoliucija (lot. *revoliutio*) - tai kokybinis gamtos, visuomenės, pažinimo reiškinių raidos pasikeitimas, perversmas[42]. Įvairūs literatūros šaltiniai mokslo bei technologijų revoliucijos raidą apibūdina kaip pramonės revoliuciją, kuri, pagal istorinius laikotarpius, skirstoma į tam tikrus etapus. Pavyzdžiui, profesorius Klaus Schwab išskiria net kelias pramonės revoliucijas: pirmąją, antrąją, trečiąją bei ketvirtąją pramonės revoliuciją[43], kurios toliau ir bus apžvelgiamos šiame darbe.

---

[41] CIVILKA, M. Asmens duomenų apsaugos teisinis reguliavimas internet kontekste [interaktyvus], p. 9, [žiūrėta 2020 m. kovo 8 d.]. Prieiga per internetą: http://media.search.lt/GetFile.php?OID=92932&FID=269994.
[42] Tarptautinių žodžių žodynas. *Alma Littera*, 2013. p. 647.
[43] SCHWAB, Klaus. The Fourth Industrial Revolution. *World Econimic Forum*, 2016, p. 7.

XVIII a. antroje pusėje žmogaus fizinį darbą pradėjo keisti įvairūs mechanizmai. Atsižvelgus į tai, pirmoji pramonės revoliucija įvyko 1760 m. ir yra siejama su mechanikos inovacijomis Anglijoje, iš kurių viena pirmųjų buvo verpimo mašinos išradimas, 1765 m. patentuotas James Hargreaves. Vienas iš svarbiausių išradimų, su kuriuo dažniausiai ir yra siejama pirmoji pramonės revoliucija yra 1769 m. James Watt sukurta garo mašina bei 1815 m. Goerge Stevenson sukonstruotas pirmasis geležinkelis. Šie išradimai paspartino industrializacijos procesą, suteikė galimybę pramonės perversmo nulemtiems pokyčiams pasklisti visame pasaulyje. Pirmoji pramonės revoliucija iš Anglijos plito į Vakarų Europą, paskui pasiekė JAV, Japoniją, Rusiją. Pirmosios pramonės revoliucijos metais (1760 m. - 1840 m.) įvyko labai svarbūs buities ir gyvenimo pokyčiai, urbanizacija, formavosi politinės srovės bei teorijos, prasidėjo darbininkų judėjimas. Pagerėjus gyvenimo sąlygoms, pasaulyje didėjo gyventojų skaičius, atsirado nauji gyventojų sluoksniai. Pažanga įvyko ir teisės srityje. 1776 m. Švedija priėmė pirmąjį pasaulyje teisės gauti oficialią informaciją įstatymą[44]. Šiuo teisės aktu buvo garantuojama visuomenės teisė gauti informaciją bei susipažinti su valstybės institucijų turimais dokumentais. Tuo tarpu, 1858 m. Prancūzijoje priėmė įstatymą, kuriuo buvo uždraustas privačių faktų skelbimas ir numatytos atitinkamos baudos už šio reikalavimo nesilaikymą. Tai buvo pirmosios asmens duomenų teisės užuomazgos, kurios stipriai įtakojo šios teisės bei "teisės į privatumą" atsiradimą ateityje.

Tolesni mokslo ir technikos išradimai davė postūmį antrosios pramonės revoliucijos pradžiai: 1860 m. buvo išrastas vidaus degimo variklis, 1876 m. išrastas telefonas, o 1879 m. Thomas Edison išrado elektros lemputę. Šių technikos išradimų dėka, pasikeitė darbo bei gyvenimo sąlygos, atsirado automatizacijos procesas ir XIX a. pabaigoje - XX a. pradžioje įvyko antroji pramonės revoliucija. Šis istorinis laikotarpis stipriai įtakojo situacijos pasikeitimą žmogaus teisių srityje. Daugybė teisės mokslininkų pradėjo aktyviai plėtoti "teisės

[44] Riksdag's (Swedish Parliament) "Access to Public Records Act", 1776.

į privatumą" sampratą. Vykstant antrajai pramonės revoliucijai, kuri toliau skatino civilizacijos vystymąsi bei tobulėjimą, visuomenei nebeužteko asmens teisių ir laisvių, kurios apgintų tik jų gyvybę, laisvę ar nuosavybę. Žmonių mintys, emocijos ir pojūčiai, taip pat, reikalavo teisinio pripažinimo. Todėl, „teisė į gyvybę" dabar reiškė ne tik teisę gyventi, bet ir teisę mėgautis gyvenimu. Toks teisės vystymasis buvo neišvengiamas antrosios pramonės revoliucijos padarinys. 1890 m. teisininkai Samuel Warren ir Louis Brandeis savo įžymiajame straipsnyje "Teisė į privatumą" pirmą kartą pabrėžė būtinybę priimti atitinkamus teisės aktus, apsaugančius asmenis nuo jų privatumo pažeidimo. Straipsnio autorių nuomone, kai informacija apie asmens privatų gyvenimą tampa prieinama kitiems, ji gali stipriai pakenkti asmeniui bei jo požiūriui į save[45]. Jie "teisę į privatumą" įvardijo kaip "teisę būti paliktam vienam"[46]. Tai reiškė asmens teisę pasirinkti ar dalintis su kitais informacija, susijusia su jų privačiu gyvenimu, pomėgiais, santykiais, ar ne. Šis straipsnis iki šiol laikomas atskaitos tašku visuotiniam "teisės į privatumą" pripažinimui bei įtvirtinimui tarptautiniuose teisės aktuose.

„Teisės į privatumą" samprata toliau buvo aktyviai plėtojama Jungtinių Amerikos Valstijų teisės mokslininkų. Alan Westin teisę į privatumą apibūdino kaip „asmens galimybę nuspręsti, kada, kokiu būdu ir kokia informacija apie jį bendraujant gali būti pateikiama kitiems[47]". Tuo tarpu, William Prosser teisę į privatumą susiejo su „asmens apsauga nuo trikdančios informacijos ir iškreiptų faktų apie asmenį paviešinimo[48]". Atsižvelgus į tai, prigimtinių žmogaus teisių samprata palaipsniui plėtėsi ir "teisė į privatumą" pirmą kartą buvo oficialiai įtvirtinta 1948 m. Visuotinėje žmogaus teisių deklaracijoje[49], kuri numatė, jog „niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą, kėsinimosi į jo garbę ir reputaciją, kad kiekvienas turi teisę į įstatymo apsaugą nuo tokio

[45] WARREN, Samuel; BRANDEIS D. Louis. *Harvard Law Review*, Vol. 4, No. 5. (Dec. 15, 1890), p. 196.
[46] *Ibid*, p. 197.
[47] WESTIN, Alan. Privacy and Freedom. New York, 1967, p.7.
[48] PROSSER, William. Privacy. *California Law Review.* 1960, No. 338, p. 389.
[49] Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006, Nr. 68-2497.

kišimosi ar kėsinimosi“. Vėliau, “teisė į privatumą” buvo įtvirtinta ir 1950 m. Europos žmogaus teisių ir laisvių apsaugos konvencijoje, kurios 8 straipsnis numato, kad: „kiekvienas turi teisę į tai, kad būtų gerbiamas asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas, kad valdžios pareigūnai neturi teisės kištis į naudojimąsi šia teise, išskyrus tam tikrus atvejus.“ Šios teisės turinys plačiau yra atskleidžiamas ir Europos žmogaus teisių teismo sprendimuose, kuriuose Teismas yra pažymėjęs, kad privataus gyvenimo sąvoka apima asmenybės raidą asmens santykiuose su kitais asmenimis asmens fizinį ir moralinį vientisumą, seksualinę orientaciją ir lytinį gyvenimą, informaciją apie asmenį ir kita[50].

XX a. antrojoje pusėje, sparčiai vystantis kompiuterinėms technologijoms, įvyko trečioji pramonės revoliucija, kurios pradžia siejama su centrinių kompiuterių sukūrimu. Pirmieji elektromechaniniai kompiuteriai buvo sukurti Vokietijoje bei JAV. Vėliau, buvo pradėti gaminti pirmieji duomenų saugojimo įrenginiai. Vienas tokių įrenginių - 1956 m. IBM sukurtas pirmasis magnetinis kietasis diskas, kuris tuo metu kainavo 50 tūkst. dolerių ir svėrė net kelias tonas.[51] Šie ir kiti panašūs išradimai paskatino informacinių technologijų plėtrą, kadangi buvo atrasti nauji būdai kaip rinkti, kaupti bei saugoti asmens duomenis. Pasitelkus naująsias technologijas, tokius duomenis buvo pradėta tvarkyti automatiniu būdu. Tokia sparti technologijų pažanga ne tik atvėrė daug naujų perspektyvų ekonominiam, socialiniam bei kultūriniam progresui, bet ir pradėjo kelti nemenką susirūpinimą. 1968 m. Teherano žmogaus teisių konferencijoje išsakyta nuomonė, jog, nepaisant to, kad tuometiniai moksliniai atradimai ir technologinė pažanga padeda civilizacijai progresuoti bei gerina gyvenimo kokybę, tai, taip pat, gali sukelti pavojų pagrindinėms žmogaus teisėms bei laisvėms[52]. Atsižvelgus į tai, atitinkamoms valstybių institucijoms buvo rekomenduota ištirti grėsmes, kurias galėjo sukelti

[50] Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*. 1995, Nr. 40-98.
[51] LEVY, Steven. The Hard Disk That Changed the World. *Newsweek*, 2006 [interaktyvus, žiūrėta 2020 m. kovo 30 d.). Prieiga per internetą: http://www.newsweek.com/hard-disk-changed-world-108939Steven Levy, "The Hard Disk That Changed the World" Newsweek, August 7, 2006.
[52] Proclamation of Tehran, Final Act of the International Conference on Human Rights, Teheran, 22 April to 13 May 1968. U.N. Doc. A/CONF. 32/41.

tokie greiti pokyčiai mokslo bei technologijų srityje, ypatingai didelį dėmesį skiriant asmenų privatumui. Svarbu paminėti, jog 1970 m. Vokietijos Heseno žemėje (vakarinėje Vokietijos Federacijos dalyje) buvo priimtas pirmasis pasaulyje asmens duomenų apsaugos įstatymas[53]. Šio įstatymo tikslas buvo sureguliuoti asmens duomenų tvarkymą ir užtikrinti, kad asmens duomenimis nebūtų piktnaudžiaujama, taip siekiant apsaugoti asmenis nuo žalos, kurią gali sukelti netinkamas jų duomenų tvarkymas. Šis teisės aktas yra ypatingai svarbus, kadangi tai buvo vienas pirmųjų bandymų sureguliuoti santykius, susijusius su asmens duomenų tvarkymu bei kovoti su pavojumi, kurį kėlė technologinė pažanga bei moksliniai atradimai, įvykę trečiosios pramonės revoliucijos metu. 1973 m. tokiu pat pavyzdžiu pasekė ir Švedija, priimdama pirmąjį pasaulyje asmens duomenų apsaugos įstatymą[54], kuris asmens duomenų tvarkymą reglamentavo nacionaliniu lygiu. 1977 m. asmens duomenų apsaugos įstatymą priėmė Vokietija, o 1978 m. asmens duomenų apsaugos įstatymus priėmė daugelis Europos šalių: Danija, Austrija, Prancūzija, Norvegija. Šie teisės aktai buvo daug kartų tobulinami bei keičiami, tačiau jie yra laikomi pirmosios kartos teisės aktais, nacionaliniu lygiu reglamentuojančiais santykius, susijusius su asmens duomenų tvarkymu.

Pastangos užtikrinti asmens duomenų apsaugą tarptautiniu lygiu, pirmą kartą buvo parodytos Privatumo gairėse. Šios gairės taikomos bet kokiai informacijai, susijusiai su asmeniu, kurio tapatybė yra nustatyta ar gali būti nustatyta. Privatumo gairės taikomos tiek privačiajam, tiek ir viešajam sektoriui, visoms kompiuterizuoto asmens duomenų tvarkymo sistemoms bei priemonėms ir apima bet kokį asmens duomenų tvarkymą ar kitokį naudojimą. Kaip jau buvo minėta, šis dokumentas pirmą kartą tarptautiniu lygmeniu susistemino bei įtvirtino pagrindinius asmens duomenų tvarkymo principus. Nors Privatumo gairės ir nebuvo teisiškai privalomos, tačiau stipriai įtakojo vėlesnį daugelio pasaulio valstybių teisinį

[53]Datenschutzgesetz (Data Protection Act), Oct.7, 1970, HESSISCHES GESETZUND VERORDNUNGSBLATT I.
[54] Sweden, *Data Protection Act*, No. 289 (1973).

reglamentavimą asmens duomenų apsaugos srityje. Tuo tarpu, atsižvelgdama į didėjantį automatizuotai tvarkomų asmens duomenų srautą bei siekdama harmonizuoti duomenų apsaugos teisę tarptautiniu lygiu, 1981 m. Europos Taryba priėmė Konvenciją Nr. 108[55]. Šiame teisės akte numatyti pagrindiniai duomenų apsaugos teisės apibrėžimai, principai, daug dėmesio skirta šalių bendradarbiavimui bei abipusei pagalbai asmens duomenų apsaugos srityje. Konvencijoje Nr. 108 nustatytos ne tik su asmens duomenų rinkimu ir tvarkymu susijusios garantijos, bet ir draudžiama tvarkyti ypatingus duomenis, pavyzdžiui: susijusius su asmens rase, politiniais įsitikinimais, sveikata, religija, lytiniu gyvenimu arba informacija apie teistumą, jeigu tokiam tvarkymui nėra taikomos tinkamos teisinės apsaugos priemonės. Šiame teisės akte, taip pat, numatyta asmens teisė žinoti, kad informacija apie jį yra saugoma, ir teisė prireikus reikalauti, kad tokia informacija būtų ištaisyta. 1981 m. pirmą kartą buvo įsteigtas konsultacinis komitetas, skirtas tobulinti bei taisyti Konvenciją Nr. 108, atsižvelgiant į interneto plėtrą bei sparčią skaitmeninių technologijų pažangą. Konvenciją Nr. 108 ratifikavo visos Europos Sąjungos valstybės narės. Lietuvoje šis teisės aktas įsigaliojo tik 2001 m. Vykstant trečiajai pramonės revoliucijai, asmens duomenų apsauga tapo prioritetu daugeliui valstybių. Tais pačiais metais Jungtinė Karalystė priėmė Duomenų apsaugos įstatymą, vėliau tokiu pat pavyzdžiu pasekė ir kitos valstybės: 1987 m. Suomija priėmė Asmens duomenų rinkmenų įstatymą, o 1988 m. Asmens duomenų apsaugos įstatymus priėmė Airija bei Australija.

Paskelbus Konvenciją Nr. 108, prireikė beveik 15 metų, kad būtų imtasi teisinių priemonių asmens duomenų apsaugai užtikrinti Europos Sąjungos lygiu. Atsižvelgus į informacinių technologijų pažangos daromą įtaką vis didėjantiems asmens duomenų keitimosi mastams, 1995 m. buvo priimta Duomenų apsaugos direktyva[56]. Tuo metu tai buvo

[55] 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Nr. 108, *Valstybės žinios*. 2001, Nr. 32-1059.
[56] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, *Specialusis leidimas*, OL L 281, p. 1-31.

pažangiausias bei išsamiausias tarptautinis teisės aktas, reglamentuojantis teisinius santykius, susijusius su asmens duomenų tvarkymu. Šiuo teisės aktu buvo siekiama suvienodinti valstybių narių nacionalinius įstatymus, reglamentuojančius asmens duomenų apsaugą bei harmonizuoti teisinį reguliavimą šioje srityje, kadangi toks reguliavimas valstybėse narėse gerokai skyrėsi, o kai kurios valstybės išvis nebuvo priėmusios jokio teisės akto, reglamentuojančio teisinius santykius, susijusius su asmens duomenų tvarkymu. Duomenų apsaugos direktyva buvo skirta apsaugoti fizinių asmenų teises ir laisves, ypač jų privatumo teisę tvarkant asmens duomenis, tuo pačiu, užtikrinti laisvą asmens duomenų judėjimą tarp valstybių narių, kuris sudarytų galimybes tolimesnei socialinei bei ekonominei valstybių narių integracijai.

Svarbu pabrėžti, kad Duomenų apsaugos direktyva buvo bendro pobūdžio teisės aktas. Atsižvelgus į tai, vėliau atsirado būtinybė priimti išsamesnius bei detalesnius teisės aktų, kuriais buvo siekiama didesnio aiškumo asmens duomenų apsaugos srityje, nustatant kitų teisėtų interesų pusiausvyrą. Siekiant nustatyti duomenų apsaugą Europos Sąjungos institucijoms ir įstaigoms tvarkant asmens duomenis buvo priimtas Reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[57]. Vėliau, buvo priimti ir šie teisės aktai: Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje[58] ir Direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB (neteko galios 2014 m. balandžio 8d.)[59]. Atitinkamai,

[57] 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo. OL L 8, 2001 1 12, p. 1-22.

[58] 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių). OL L 201, 2002 7 31, p. 37–47.

[59] 2006 m. kovo 15 d. Europos Parlamento ir Tarybos direktyva 2006/24/EB dėl duomenų, generuojamų arba tvarkomų teikiant viešai prieinamas elektroninių ryšių paslaugas arba viešuosius ryšių tinklus, saugojimo ir iš dalies keičianti Direktyvą 2002/58/EB OJ L 105, 13.4.2006, p. 54–63

teisė į asmens duomenų apsaugą buvo pripažinta ir išskirta kaip atskira teisė 2007 m. Lisabonos sutartyje[60] bei Europos Sąjungos pagrindinių teisių chartijoje[61].

Ir toliau sparčiai tobulėjant informacinėms technologijoms bei plečiantis skaitmeninei rinkai, pradėta kalbėti apie ketvirtosios pramonės revoliucijos pradžią. Pirmą kartą ši sąvoka buvo paminėta 2011 m. Vokietijoje, Hanoverio mugėje. Ketvirtoji pramonės revoliucija yra naujas ekonomikos raidos etapas, apibrėžiamas kaip „naujausių ir dažnai tarpusavyje susietų skaitmeninių technologijų, kurios įgalina naujus ir efektyvesnius procesus ir kai kuriais atvejais sukuria naujas prekes ir paslaugas, naudojimą pramoninėje gamyboje[62].“ O tokių skaitmeninių technologijų yra daug: pradedant mašininiu mokymusi (ang. *machine learning*) ir didžiųjų duomenų (ang. *Big data*) analize, suteikiančia galimybių tobulėti dirbtiniam intelektui ir baigiant daiktų internetu (ang. *Internet of Things*), “blockchain” technologija bei naujais valdymo prietaisais, kurie suteikia galimybę antrosios kartos pramoninei robotikai[63]. Svarbu pabrėžti, kad nuo pirmųjų trijų pramonės revoliucijų naujoji revoliucija skiriasi, pirmiausia, savo greičiu, eksponentiniu plėtojimusi, antra, savo plačia įvairove, apimančia tiek ekonomikos, tiek verslo, visuomenės ir paties žmogaus paradigmų pokyčius ir, trečia, sistemų transformacijomis, apimančios valstybių, įmonių, pramonės sektorių ir visos visuomenės sistemų pertvarką[64].

Sparčiai didėjant asmens duomenų tvarkymo mastams bei plečiantis skaitmeninei rinkai, pasitikėjimas Duomenų apsaugos direktyva smarkiai sumažėjo, iškilo abejonių dėl tolimesnio asmens duomenų apsaugos užtikrinimo naujųjų technologijų amžiuje. Atsirado

[60] Lisabonos sutartis, iš dalies keičianti Europos Sąjungos sutartį ir Europos bendrijos steigimo sutartį. OL C 306, 2007 12 13, p. 1-273.
[61] Europos Sąjungos pagrindinių teisių chartija. OL C 326, 2012 10 26, p. 391-407.
[62]Organisation for Economic Co-operation and Development (OECD). The Next Production Revolution Implications for Governments and Business, 2017, p. 27.
[63] *Ibid*., p. 28.
[64] SCHWAB, Klaus.*The Fourth Industrial Revolution: What It Means and How to Respond*, Foreign affairs, 2015 [interaktyvus, žiūrėta 2020 m. kovo 28 d.]. Prieiga per internetą: https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.

būtinybė suvienodinti ir sugriežtinti teisinį reguliavimą bei išplėsti duomenų subjektų teises asmens duomenų apsaugos srityje. Dėl šios priežasties, 2016 m. balandžio 27 d. Europos Sąjunga priėmė Bendrąjį duomenų apsaugos reglamentą (pradėtas taikyti 2018 m. gegužės 25 d.), kuris bus plačiau aptariamas sekančiame skyriuje.

Atsižvelgus į tai, kas išdėstyta, galima teigti, jog XIX a. pabaigoje prasidėjusi antroji pramonės revoliucija paskatino „teisės į privatumą“ kaip savarankiškos žmogaus teisės visuotinį pripažinimą ir įtvirtinimą tarptautiniuose teisės aktuose, o XX a. antrojoje pusėje, prasidėjus trečiajai pramonės revoliucijai bei vykstant reikšmingiems pokyčiams mokslo ir technologijų srityje, pilnai susiformavo asmens duomenų apsaugos teisės koncepcija.

2. ES BENDRASIS DUOMENŲ APSAUGOS REGLAMENTAS KAIP KETVIRTOSIOS PRAMONĖS REVOLIUCIJOS TECHNOLOGIJŲ REGULIAVIMO ŠALTINIS

2.1. ES Bendrojo duomenų apsaugos reglamento reikšmė ir pagrindiniai tikslai

Kaip jau buvo minėta, 2018 m. gegužės 25 d. Europos Sąjungoje buvo pradėtas taikyti Bendrasis duomenų apsaugos reglamentas, kuris pakeitė Duomenų apsaugos direktyvą. Viena pagrindinių priežasčių, lemiančių šio teisės akto atsiradimą buvo sparti technologinė pažanga bei globalizacija. Technologijos įtakojo ekonominę ir socialinę integraciją, todėl, stipriai išaugo asmens duomenų rinkimo bei keitimosi jais mastas. Fiziniai asmenys vis dažniau viešino savo asmeninę informaciją pasauliniu mastu, o naujausios technologijos suteikė galimybę Europos Sąjungoje veikiančioms privačioms įmonėms ir valdžios institucijoms naudotis asmens duomenimis precedento neturinčiais mastais.[65] Pabrėžtina, jog ketvirtosios pramonės revoliucijos technologijos turi vieną bendrą bruožą - jas įgalino informacinės technologijas bei informacija[66]. Šios technologijos yra paremtos didžiuliais duomenų kiekiais, kurie yra jų varomoji galia. Neveltui profesorius Klaus Schwab ketvirtosios pramonės revoliucijos pasaulį vadina duomenų pasauliu[67].

Ketvirtosios pramonės revoliucijos technologijos, tokios kaip dirbtinis intelektas, didžiųjų duomenų analizė ar daiktų internetas patenka į duomenų apsaugos reguliavimo apimtį, kadangi, rinkdamos informaciją apie fizinį pasaulį, jo objektus bei reiškinius, vienokiu ar kitokiu būdu renka bei tvarko ir asmens duomenis, t.y. bet kokią informaciją apie fizinį asmenį, kurio tapatybė yra nustatyta ar kurio tapatybę galima nustatyti[68]. Numatoma, jog ketvirtoji

[65] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 318.
[66] *Ibid*., p. 319.
[67] SCHWAB, Klaus, DAVIS, Nicholas. The shaping of Fourth Industrial Revolution. *Portfolio Penguin*, 2018, p. 19-22.
[68] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.

pramonės revoliucija atskleis maksimalų asmeninės informacijos kiekį, kokį kada nors matė pasaulis[69]. Dėl šios priežasties, asmens duomenų apsauga bei privatumas išlieka vienu svarbiausių iššūkių.

Svarbu paminėti, jog Bendrasis duomenų apsaugos reglamentas nenustato jokių specialių taisyklių minėtoms ketvirtosios pramonės revoliucijos technologijoms. Nepaisant to, šis teisės aktas yra taikomas visoms šioms technologijoms net ir be specialaus teisinio reguliavimo, kadangi yra neutralus technologijų atžvilgiu ir nepriklauso nuo duomenų tvarkymo metodų (Bendrojo duomenų apsaugos reglamento preambulės 15 p.). Būtent dėl technologinio neutralumo principo, įtvirtinto Bendrajame duomenų apsaugos reglamente, užtikrinamas asmens duomenų apsaugos teisės tęstinumas toliau vykstant ketvirtajai pramonės revoliucijai, įskaitant jo taikymą dar nesukurtoms technologijoms[70]. Bendruoju duomenų apsaugos reglamentu siekiama užtikrinti laisvą bei saugų asmens duomenų judėjimą Europos Sąjungoje bei sustiprinti duomenų subjektų apsaugą nuo ketvirtosios pramonės revoliucijos technologijų keliamų pavojų. Kitaip tariant, šis teisės aktas sukurtas kaip atsakas į vis didėjantį asmens duomenų tvarkymo mastą, kurį įgalino naujausios technologijos ir kuris gali sukelti itin neigiamus padarinius duomenų subjektams.

Kita priežastis, lemianti Bendrojo duomenų apsaugos reglamento atsiradimą, buvo nevienodas Duomenų apsaugos direktyvos interpretavimas bei įgyvendinimas Europos Sąjungoje. Kitaip nei Bendrasis duomenų apsaugos reglamentas, kuris Europos Sąjungos valstybėms narėms yra taikomas tiesiogiai ir įgyvendinamas tuoj pat po jo įsigaliojimo, Duomenų apsaugos direktyva Europos Sąjungos valstybėse narėse nebuvo taikoma tiesiogiai.

[69] ONIK, Mehedi Hassan; KIM, Chul-Soo; YANG, Jinhong. Personal Data Privacy Challenges of the Fourth Industrial Revolution. *International Conference on Advanced Communications Technology (ICACT)*, Conference Paper, February 2019, p. 635.
[70] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 322.

Atsižvelgus į direktyvos[71] apibrėžimą, šiuo teisės aktu yra nustatomas tikslas, kurį visos Europos Sąjungos valstybės narės privalo pasiekti, tačiau kiekviena valstybė narė turi teisę pasirinkti kaip ir kokiomis priemonėmis šį tikslą įgyvendins. Akivaizdu, kad valstybės narės tokį teisės aktą gali skirtingai suprasti ir interpretuoti, todėl tos pačios direktyvos įgyvendinimas bei taikymas valstybėse narėse gali žymiai skirtis. Duomenų apsaugos direktyva neužkirto kelio suskaidytam duomenų apsaugos įgyvendinimui Europos Sąjungoje, teisiniam netikrumui ar plačiai paplitusiai viešajai nuomonei, kad fizinių asmenų apsaugai kyla didelių pavojų, visų pirma dėl veiklos internete (Bendrojo duomenų apsaugos reglamento preambulės 9 p.). Kadangi asmens duomenų apsaugos lygis valstybėse narėse skyrėsi, tai trukdė laisvam asmens duomenų judėjimui Europos Sąjungoje, iškilo kliūtys užsiimti ekonomine veikla, atsirado iškreiptos konkurencijos pavojus. Duomenų apsaugos direktyvoje numatytas teisinis reglamentavimas tapo per daug abstraktus ir neužtikrino tinkamos duomenų subjektų teisių apsaugos, o tai kėlė didelį susirūpinimą bei nepasitikėjimą šiuo teisės aktu. Atsižvelgus į gresiančius pavojus asmens duomenų apsaugos srityje, atsirado būtinybė suvienodinti teisinį reguliavimą visoje Europos Sąjungoje.

Svarbu pabrėžti, jog Bendrojo asmens duomenų reglamento pagrindinis tikslas užtikrinti vienodo lygio fizinių asmenų apsaugą visoje Europos Sąjungoje ir neleisti atsirasti skirtumams, kurie kliudo laisvam asmens duomenų judėjimui vidaus rinkoje (Bendrojo duomenų apsaugos reglamento preambulės 13 p.). Šiuo teisės aktu yra saugomos fizinių asmenų pagrindinės teisės ir laisvės, o visų pirma jų teisė į asmens duomenų apsaugą[72]. Kad šie tikslai būtų tinkamai įgyvendinti, Bendrajame duomenų apsaugos reglamente nustatomos taisyklės, susijusios su fizinių asmenų apsauga tvarkant jų asmens duomenis, ir taisyklės,

[71] Direktyva – teisės aktas, privalomas kiekvienai valstybei narei, kuriai jis skirtas, rezultato, kurį reikia pasiekti, atžvilgiu, bet nacionalinės valdžios institucijos pačios pasirenka direktyvos įgyvendinimo formą ir būdus.
[72] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.

susijusios su laisvu asmens duomenų judėjimu. Palyginus su Duomenų apsaugos direktyva, Bendrajame duomenų apsaugos reglamente konkrečiau apibrėžtos asmens duomenų apsaugos taisyklės, nustatytos griežtesnės sankcijos už asmens duomenų apsaugos pažeidimus, sustiprintos bei išplėstos duomenų subjektų teisės, numatyta duomenų valdytojų ir duomenų tvarkytojų atsakomybė bei užtikrintas duomenų apsaugos reglamentavimo skaidrumas ir teisinis tikrumas. Šiuo atžvilgiu, Bendrąjį duomenų apsaugos reglamentą galima traktuoti kaip asmens duomenų apsaugos teisės reformos Europos Sąjungoje rezultatą, skatinantį duomenų apsaugos teisės globalizaciją bei verslo plėtrą[73].

Atsižvelgus į tai, kas išdėstyta, galima teigti, jog Bendrasis duomenų apsaugos reglamentas šiuo metu yra pagrindinis asmens duomenų apsaugos šaltinis, siekiantis užtikrinti aukšto lygio asmens duomenų apsaugą visoje Europos Sąjungoje bei apsaugoti duomenų subjektų teises nuo ketvirtosios pramonės revoliucijos technologijų keliamų pavojų. Sugriežtindamas asmens duomenų apsaugos teisinį reguliavimą bei išplėtęs duomenų subjektų teises, šis teisės aktas iš esmės keičia požiūrį į asmens duomenų apsaugą.

2.2. Asmens duomenų apsaugos naujovės ES Bendrajame duomenų apsaugos reglamente

Bendrajame duomenų apsaugos reglamente atnaujintas asmens duomenų apsaugos teisinis reguliavimas ir kartu įtvirtinti nauji pakeitimai, kuriais sustiprinamos duomenų subjektų teisės, atsižvelgiant į ketvirtosios pramonės revoliucijos technologijų keliamus pavojus asmens duomenų apsaugai. Kaip jau minėta, Bendrasis duomenų apsaugos reglamentas, kitaip nei prieš tai galiojusi Duomenų apsaugos direktyva, yra privalomas visa apimtimi ir taikomas tiesiogiai visose Europos Sąjungos valstybėse narėse, o tai reiškia jog šis teisės aktas neprivalo būti perkeltas į nacionalinę valstybių narių teisę. Šiuo atžvilgiu, Europos

[73] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 54.

Sąjungoje užtikrinamas vienodas asmens duomenų apsaugos taisyklių taikymas. Visos valstybės narės privalo atitikti numatytą teisinį reguliavimą, o duomenų valdytojai ar tvarkytojai pasirūpinti, kad būtų atnaujinta reikiama vidinė asmens duomenų tvarkymo sistema, atsižvelgiant į Bendrajame duomenų apsaugos reglamente nurodytus reikalavimus[74].

Viena didžiausių naujovių Bendrajame duomenų apsaugos reglamente yra šio teisės akto teritorinės taikymo srities išplėtimas. Pabrėžtina, kad Bendrasis duomenų apsaugos reglamentas yra taikomas ne tik tuo atveju, kai asmens duomenys yra tvarkomi Europos Sąjungoje įsteigto duomenų valdytojo arba duomenų tvarkytojo, bet ir tuo atveju, kai Europos Sąjungoje esančių duomenų subjektų asmens duomenys yra tvarkomi Europos Sąjungoje neįsisteigusio duomenų valdytojo ar duomenų tvarkytojo, kai duomenų tvarkymo veikla yra susijusi su prekių arba paslaugų siūlymu duomenų subjektams Europos Sąjungoje arba elgesio, kai jie veikia Europos Sąjungoje, stebėsena. Ši naujovė svarbi tuo, jog Bendruoju duomenų apsaugos reglamentu garantuojama asmens duomenų apsauga net už Europos Sąjungos ribų, taip siekiant užtikrinti itin aukšto lygio asmens duomenų apsaugos teisinį reguliavimą bei įtvirtinamos vienodos sąlygos visoms Europos Sąjungos rinkoje veiklą vykdančioms įmonėms.

Pabrėžtina, jog Bendruoju duomenų apsaugos reglamentu, taip pat išplečiamos duomenų subjektų teisės. Šiame teisės akte įtvirtinamos naujos duomenų subjektų teisės, tokios kaip: teisė susipažinti su asmens duomenimis, „teisė būti pamirštam“ (reikalauti ištrinti asmens duomenis) bei duomenų perkeliamumo teisė, pagal kurią duomenų subjektai gali reikalauti sugrąžinti jiems suteiktus asmens duomenis, kurie pateikti jų sutikimu arba vykdant sutartį, o, taip pat, leidžiama tokius asmens duomenis tiesiogiai persiųsti kitam duomenų valdytojui arba tvarkytojui, kai tai techniškai įmanoma[75]. Šios duomenų subjekto teisės bus plačiau aptartos sekančiame skyriuje.

[74] ŠTAREIKĖ, Eglė. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. *Visuomenės saugumas ir viešoji tvarka*. Mokslinių straipsnių rinkinys, 2018 (20), p. 298.
[75] Komisijos komunikatas Europos Parlamentui ir Tarybai. *Keitimasis asmens duomenimis ir jų apsauga globalizuotame pasaulyje*. COM 2017 (7) final.

Bendruoju duomenų apsaugos reglamentu sugriežtinami reikalavimai dėl duomenų subjekto sutikimo tvarkyti jo asmens duomenis. Naujomis nuostatomis įtvirtinama duomenų valdytojo pareiga įrodyti asmens duomenų tvarkymo teisėtumą. Kitaip tariant, duomenų valdytojas privalo įrodyti, kad duomenų subjektas davė sutikimą asmens duomenų tvarkymui ir, kad toks sutikimas yra gautas teisėtais pagrindais. Apskritai, sutikimas gali būti tinkamas teisėtas duomenų tvarkymo pagrindas tik tada, kai duomenų subjektui suteikiama kontrolė ir suteikiama reali galimybė rinktis sutikti arba nesutikti su siūlomomis sąlygomis ar jų atsisakyti nepatiriant žalos[76]. Šiuo atžvilgiu, duomenų subjekto neveikimas arba tyla nebeprilyginami duomenų subjekto sutikimui tvarkyti jo asmens duomenis. Svarbu, jog duomenų subjektas tokį sutikimą tvarkyti jo asmens duomenis duotų laisva valia, o toks valios išreiškimas būtų, nedviprasmiškas ir patvirtintas pareiškimu ar konkrečiais veiksmais. Atitinkamai, turi būti užtikrinama, kad duomenų subjektas suvoktų, jog jis duoda sutikimą tvarkyti jo asmens duomenis ir kokiais tikslais jis jį duoda. Atsižvelgus į tai, duomenų valdytojo iš anksto suformuluotas sutikimo pareiškimas privalo būti pateiktas suprantama ir lengvai prieinama forma, aiškiai ir paprasta kalba. Duomenų subjektui, taip pat, turi būti nurodyta, jog jis bet kuriuo metu turi teisę atšaukti sutikimą tvarkyti jo asmens duomenis.

Atkreiptinas dėmesys, kad sugriežtinti reikalavimai bei numatytos naujos pareigos duomenų valdytojams, tvarkantiems nepilnamečių asmens duomenis. Bendrojo duomenų apsaugos reglamento 8 straipsnis numato jog, „kai vaikas yra jaunesnis nei 16 metų, jo asmens duomenų tvarkymas yra teisėtas tik tokiu atveju, jei sutikimą davė ar tvarkyti duomenis leido vaiko tėvų pareigų turėtojas, ir tik Tokiu mastu kokiu duotas sutikimas ar leidimas, o vaikui tapus suaugusiu, jis įgyja teisę tokį suteikimą ar leidimą atšaukti.“ Kitaip tariant, duomenų valdytojas, jokiais būdais, neturi teisės tvarkyti nepilnamečio iki 16 m. asmens duomenis, jei

[76] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. Gairės dėl sutikimo pagal Reglamentą 2016/679*, WP259 red. 01, 17/LT, p. 11.

nėra suteiktas tėvų ar globėjų sutikimas. Šis pakeitimas yra labai svarbus šiuolaikinių technologijų amžiuje. Vaikų asmens duomenims yra būtina ypatinga apsauga, kadangi jie gali nepakankamai suvokti gresiančius pavojus bei neigiamus padarinius, kuriuos jiems gali sukelti asmens duomenų tvarkymas. Minėtų reikalavimų sugriežtinimu, siekiama daugiau skaidrumo asmens duomenų apsaugos srityje.

Bendrajame duomenų apsaugos reglamente užtikrinama efektyvesnė apsauga nuo bet kokių asmens duomenų saugumo pažeidimų, kurie gali stipriai pakenkti fiziniams asmenims. Bendrojo duomenų apsaugos reglamento preambulės 85 dalyje nurodyta, jog: „dėl asmens duomenų saugumo pažeidimo, jei dėl jo laiku nesiimama tinkamų priemonių, fiziniai asmenys gali patirti kūno sužalojimą, materialinę ar nematerialinę žalą, pavyzdžiui, prarasti savo asmens duomenų kontrolę, patirti teisių apribojimą, diskriminaciją, gali būti pavogta ar suklastota jo asmens tapatybė, jam padaryta finansinių nuostolių, neleistinai panaikinti pseudonimai, gali būti pakenkta jo reputacijai, prarastas asmens duomenų, kurie saugomi profesine paslaptimi, konfidencialumas arba padaryta kita ekonominė ar socialinė žala atitinkamam fiziniam asmeniui.“ Atsižvelgus į tai, šiame teisės akte nustatytos specialios procedūros bei reikalavimai siekiant išvengti minėtų padarinių. Vienas pagrindinių reikalavimų – duomenų valdytojo ar tvarkytojo pareiga informuoti priežiūros instituciją apie asmens duomenų saugumo pažeidimą ne vėliau kaip per 72 valandas, jeigu toks asmens duomenų saugumo pažeidimas gali kelti pavojų fizinių asmenų teisėms[77]. Palyginus su ankstesniu teisiniu reguliavimu, tokią pareigą turėjo tik elektroninių ryšių ar skaitmeninių paslaugų teikėjai.

Svarbu paminėti, jog Bendrajame duomenų apsaugos reglamente numatyta ir duomenų tvarkytojo atsakomybė už savo pareigų nevykdymą arba duomenų valdytojo nurodymų nesilaikymą. Dar daugiau, tais atvejais, kai su tuo pačiu duomenų tvarkymo atveju yra susiję

[77] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.

keli duomenų valdytojai ir (ar) tvarkytojai, reglamentas numato solidarią visų jų atsakomybę, t.y. duomenų subjekto teisę visos žalos atlyginimo reikalauti tiek iš duomenų valdytojo, tiek iš duomenų tvarkytojo. Tokiu būdu išplečiamos duomenų tvarkytojo pareigos asmens duomenų apsaugos srityje.

Kita svarbi naujovė – už netinkamą asmens duomenų saugumo pažeidimus bei Bendrojo duomenų apsaugos reglamento nuostatų nesilaikymą numatomos įspūdingo dydžio sankcijos. Tinkamai nesilaikius Bendrojo duomenų apsaugos reglamento nuostatų, duomenų valdytojams gali būti skiriamos veiksmingos, proporcingos, tačiau atgrasančios baudos. Šių baudų dydis priklauso nuo pažeidimo pobūdžio, sunkumo ir trukmės, atsižvelgiant į atitinkamo duomenų tvarkymo pobūdį ar tikslą, taip pat į nukentėjusių duomenų subjektų skaičių ir jų patirtos žalos dydį. Minėtos baudos dydis gali siekti iki 20 mln. eurų arba 4 proc. ankstesnių finansinių metų bendros metinės pasaulinės apyvartos. Negana to, Bendrojo duomenų apsaugos reglamento reikalavimus pažeidusiems duomenų valdytojams ir tvarkytojams, taip pat, gali tekti atlyginti ir dėl tokio pažeidimo duomenų subjekto patirtą turtinę bei neturtinę žalą. 2019 m. sausio 21 d. pirma solidi bauda buvo skirta interneto gigantei „Google“ už ilgą laiką besitęsiančius Bendrojo duomenų apsaugos reglamento pažeidimus. Prancūzijos duomenų apsaugos tarnyba nustatė, jog „Google“, veikdama kaip duomenų valdytojas, neužtikrino tinkamo duomenų subjektų informavimo apie asmens duomenų rinkimą, taip pat rinko bei tvarkė savo vartotojų asmens duomenis, negavus teisėto vartotojų sutikimo specifiniam asmens duomenų tvarkymui (vartotojai matė suasmenintas reklamas)[78]. Atsižvelgus į tai, galima teigti, jog numatytų sankcijų pagalba siekiama užtikrinti efektyvesnę asmens duomenų apsaugos teisinio reguliavimo įgyvendinimo kontrolę.

[78] Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC, p. 27.

Dar viena naujovė asmens duomenų apsaugos teisės srityje – reikalavimas tam tikriems duomenų valdytojams ir tvarkytojams paskirti duomenų apsaugos pareigūną, kuris stebi duomenų valdytojų bei tvarkytojų veiklą, informuoja apie jų pareigas, konsultuoja ir apmoko darbuotojus, konsultuoja duomenų valdytoją bei tvarkytoją dėl poveikio duomenų apsaugai vertinimo atlikimo, komunikuoja su duomenų subjektais bei bendradarbiauja su duomenų apsaugos priežiūros institucijomis[79]. Naujuoju reikalavimu siekiama sustiprinti pasitikėjimą duomenų valdytojais bei tvarkytojais, tuo pačiu, labiau užtikrinami asmens duomenų tvarkymui keliami reikalavimai. Pažymėtina, kad duomenų apsaugos pareigūnui yra suteikiama autonomija ir visiškas nepriklausomumas, t.y. duomenų valdytojas ir duomenų tvarkytojas turi užtikrinti, kad duomenų apsaugos pareigūnas negautų nurodymų dėl savo funkcijų vykdymo ir, kad jam nebūtų daroma įtaka, siekiant nesilaikyti duomenų tvarkymą nustatančių reikalavimų. Bendrasis duomenų apsaugos reglamente įtvirtinta duomenų valdytojo ir duomenų tvarkytojo pareiga užtikrinti, jog duomenų apsaugos pareigūnas būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą[80], tuo tarpu duomenų apsaugos pareigūno pagrindinės funkcijos konsultuoti duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie Bendrojo duomenų apsaugos reglamento reikalavimus, stebėti atitiktį ir rūpintis tokios atitikties auditais.

2.3. Teritorinė ES Bendrojo duomenų apsaugos reglamento taikymo sritis

Kaip jau minėta, Bendrajame duomenų apsaugos reglamente yra išplėsta teritorinė šio teisės akto taikymo sritis. Bendrojo duomenų apsaugos reglamento 3 straipsnis atspindi įstatymų leidėjo ketinimą užtikrinti visapusišką duomenų subjektų teisių apsaugą ir,

[79] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4.
[80] *Ibid*, 38 str. 1 d.

atsižvelgiant į duomenų apsaugos reikalavimus, nustatyti vienodas konkurencijos sąlygas Europos Sąjungos rinkoje veikiančioms įmonėms, atsižvelgiant į vis didėjantį asmens duomenų rinkimo bei keitimosi jais mastą, kurį įtakojo sparti ketvirtosios pramonės revoliucijos technologijų plėtra[81]. Dėl šios priežasties, Bendrajame duomenų apsaugos reglamente sudarytos palankesnės sąlygos laisvam asmens duomenų judėjimui Europos Sąjungoje bei jų perdavimui į trečiąsias valstybes. Nors Bendrasis duomenų apsaugos reglamentas apsaugo tik Europos Sąjungos piliečius, jo poveikis yra globalus, nes jis paveikia bet kurią įmonę ar organizaciją, kuri vykdo savo veiklą Europos Sąjungoje arba teikia prekes bei paslaugas ir tvarko asmeninę informaciją apie Europos Sąjungos gyventojus[82].

Bendrajame duomenų apsaugos reglamente numatytos trys pagrindinės sąlygos, pagal kurias yra taikomas šis teisės aktas. Visų pirma, Bendrasis duomenų apsaugos reglamentas yra taikomas asmens duomenų tvarkymui duomenų valdytojo arba tvarkytojo buveinės Europos Sąjungos veikloje, neatsižvelgiant į tai, ar duomenys tvarkomi Europos Sąjungoje, ar ne[83]. Tai reiškia, jog šis teisės aktas yra taikomas duomenų valdytojams ar tvarkytojams, kurie turi buveinę Europos Sąjungoje, nepaisant to ar jų veikla yra vykdoma tik Europos Sąjungoje ar ir už jos ribų. Todėl, pirmiausia reikia nustatyti, kad duomenų valdytojas ar tvarkytojas turi buveinę Europos Sąjungoje. Bendrasis duomenų apsaugos reglamentas nepateikia „nuolatinės buveinės“ sąvokos apibrėžimo. Nepaisant to, Bendrajame duomenų apsaugos reglamente nurodyta, jog buveinė reiškia „veiksmingą ir realią veiklą, vykdomą per stabilias struktūras.“ Teisinė tokių struktūrų forma, neatsižvelgiant į tai, ar tai filialas ar dukterinė bendrovė, turinti juridinio asmens statusą, nėra lemiamas veiksnys (Bendrojo duomenų apsaugos reglamento preambulės 22 p.). „Buveinės“ sąvoka plačiau apibrėžiama Europos Sąjungos Teisingumo

[81] European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.1, 12 November 2019, p. 3.
[82] LI, He; YU, Lu; HE, Wu. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 2019, VOL. 22, NO. 1, p. 2.
[83] *Ibid*., 3 str. 1 d.

Teismo sprendimuose, kuriuose nukrypstama nuo formalaus požiūrio, pagal kurį įmonė turėtų būti įsteigta tik savo registracijos vietoje. Šiuo atžvilgiu pirmiausia reikia pažymėti, kad Bendrasis duomenų apsaugos reglamentas taikomas duomenų valdytojui ar tvarkytojui, jei jis, per buveinę kitos valstybės narės teritorijoje, vykdo bent minimalią veiklą, kurios pagrindu atliekamas asmens duomenų tvarkymas[84]. Siekiant nustatyti, ar duomenų valdytojas ar tvarkytojas turi buveinę kitoje nei jo registracijos valstybė narė ar trečioji šalis valstybėje narėje, reikia įvertinti tiek tokio vieneto pastovumo laipsnį, tiek tai, kiek realiai yra vykdoma veikla toje kitoje valstybėje narėje atsižvelgiant į specifinį atitinkamos ekonominės veiklos ir atitinkamų paslaugų pobūdį[85]. Šis aspektas ypač svarbus įmonėms, teikiančioms paslaugas internetu, kadangi tokio pobūdžio įmonių pasaulyje vis daugėja. Pažymėtina, kad tokiais atvejais gali pakakti vieno atstovo siekiant konstatuoti, kad nuolatinis vienetas egzistuoja kitoje valstybėje narėje, jeigu to atstovo vykdoma veikla yra pakankamai pastovi, ir jei jis turi visas būtinas priemones konkrečioms paslaugoms teikti. Svarbu ne tai, kad atitinkamą asmens duomenų tvarkymą atliktų „pats“ duomenų valdytojo ar tvarkytojo padalinys, o tai, kad tvarkymas būtų atliekamas šiam padaliniui vykdant veiklą[86].

Tam tikrais atvejais juridinio asmens nuolatinės buveinės nebuvimas Europos Sąjungoje nebūtinai reiškia, kad trečiojoje šalyje įsisteigusiam duomenų valdytojui ar duomenų tvarkytojui nebus taikomas Bendrasis duomenų apsaugos reglamentas. Šio teisės akto 3 straipsnio 2 dalyje nurodomos aplinkybės, kuriomis Bendrasis duomenų apsaugos reglamentas gali būti taikomas duomenų valdytojams ar duomenų tvarkytojams, neįsisteigusiems Europos Sąjungoje, atsižvelgiant į jų vykdomą veiklą. Kaip jau buvo minėta, Bendrasis duomenų apsaugos reglamentas taikomas tokiam asmens duomenų tvarkymui, kai Europos Sąjungoje

[84] Europos Sąjungos Teisingumo Teismo 2015 m. spalio 1 d. sprendimas byloje C-230/14, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, 31 punktas.
[85] *Ibid*., 29 punktas.
[86] Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas byloje C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 52 punktas.

esančių duomenų subjektų asmens duomenis tvarko Europos Sąjungoje neįsisteigęs duomenų valdytojas arba tvarkytojas ir duomenų tvarkymo veikla yra susijusi su prekių arba paslaugų siūlymu Europos Sąjungos duomenų subjektams ar elgesio stebėsena Europos Sąjungos duomenų subjektams veikiant Europos Sąjungoje[87]. Svarbu įsitikinti, jog toks duomenų valdytojas ar tvarkytojas numato ar ketina teikti paslaugas duomenų subjektams vienoje ar keliose Europos Sąjungos valstybėse narėse. Kitaip tariant, duomenų valdytojas ar tvarkytojas turi būti pareiškęs apie savo tikslą užmegzti prekybos ryšius su duomenų subjektais iš vienos ar kelių skirtingų Europos Sąjungos valstybių narių.

Šiuo atveju, turi būti atsižvelgiama į tam tikrus veiksnius, iš kurių būtų aišku, kad duomenų valdytojas ar tvarkytojas ketina siūlyti prekes ar paslaugas duomenų subjektams Europos Sąjungoje. Kadangi vien tik to, kad Europos Sąjungoje yra prieinami duomenų valdytojo, duomenų tvarkytojo ar tarpininko interneto svetainė ar el. pašto adresas, ir kiti kontaktiniai duomenys arba kad vartojama kalba, kuri paprastai vartojama trečiojoje valstybėje, kurioje yra įsisteigęs duomenų valdytojas ar tvarkytojas, nepakanka įsitikinti, kad esama tokio ketinimo, svarbu atsižvelgti į tokius veiksnius kaip kalbos ar valiutos naudojimas, kai duomenų subjektai gali užsisakyti prekes ar paslaugas ta kalba, kurią paprastai naudoja savo šalyje. Tokį ketinimą gali rodyti ir duomenų valdytojo ar tvarkytojo veiklos pobūdis, telefono numerių su tarptautiniu kodu nurodymas, pavyzdžiui „.de“, aukščiausio lygio domeno vardo naudojimas arba neutralių aukščiausio lygio domeno vardų, kaip „.com“ ar „.eu“ naudojimas duomenų valdytojo ar tvarkytojo interneto svetainėje, taip pat, informacijos apie vartotojus, gyvenančius įvairiose Europos Sąjungos valstybėse narėse, pateikimas[88]. Kai kurie iš aukščiau išvardytų veiksnių, atskirai, gali ir nereikšti, jog duomenų valdytojas ar tvarkytojas

[87] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.
[88] Europos Sąjungos Teisingumo Teismo 2010 m. gruodžio 7 d. sprendimas byloje Peter Pammer prieš Reederei Karl Schlüter GmbH & Co KG (C-585/08), Hotel Alpenhof GesmbH prieš Oliver Heller (C-144/09), 83 punktas.

ketina teikti prekes ar paslaugas duomenų subjektams Europos Sąjungoje, tačiau reikėtų atsižvelgti į kiekvieną iš jų bei atlikti konkrečią analizę, siekiant nustatyti, ar minėti veiksniai, susiję su duomenų valdytojo ar tvarkytojo komercine veikla, kartu gali būti laikomi prekių ar paslaugų, skirtų duomenų subjektams Europos Sąjungoje, pasiūlymu[89].

Svarbu pabrėžti, kad Bendrasis duomenų apsaugos reglamentas taip pat taikomas duomenų subjektų asmens duomenų, kuriuos tvarko Europos Sąjungoje neįsisteigęs duomenų valdytojas arba duomenų tvarkytojas, tvarkymui, kai duomenų tvarkymas susijęs su tokių duomenų subjektų elgesio stebėsena. Atsižvelgus į tai, galima išskirti du kriterijus, pagal kuriuos vertinama ar šiuo atveju bus taikomas Bendrasis duomenų apsaugos reglamentas. Visų pirma, elgesio stebėjimas turi būti susijęs su duomenų subjektu, esančiu Europos Sąjungoje, o pats stebimas elgesys turi vykti Europos Sąjungos teritorijoje. Siekiant nustatyti, ar duomenų tvarkymo veikla gali būti laikoma duomenų subjektų elgesio stebėsena, svarbu įsitikinti, ar fiziniai asmenys internete gali būti atsekami, be kita ko, vėliau galbūt taikant asmens duomenų tvarkymo metodus, kuriais fiziniam asmeniui suteikiamas profilis, ypač siekiant priimti su juo susijusius sprendimus arba išnagrinėti ar prognozuoti jo asmeninius pomėgius, elgesį ir požiūrius (Bendrojo duomenų apsaugos reglamento preambulės 24 p.). Pažymėtina, jog duomenų subjektų elgesio stebėsena apima gana platų stebėjimo veiklos spektrą, pavyzdžiui: duomenų subjektų stebėjimą internete naudojant slapukus ar kitus stebėjimo metodus rinkodaros tikslais, individualizuotos dietos ir sveikatos analizės paslaugas internete, vaizdo stebėjimo sistemą (CCTV), rinkos ir kitus elgesio tyrimus, pagrįstus individualiais profiliais, duomenų subjektų sveikatos būklės stebėjimą[90].

Bendrasis duomenų apsaugos reglamentas taikomas ir tokiam asmens duomenų tvarkymui, kai asmens duomenis tvarko duomenų valdytojas ar tvarkytojas, įsisteigęs ne

[89] European Data Protection Board. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). Version 2.1, 12 November 2019, p. 14.
[90] *Ibid*, p 15.

Sąjungoje, o vietoje, kurioje pagal viešąją tarptautinę teisę taikoma valstybės narės teisė. Šiuo atžvilgiu, kalbama apie asmens duomenų tvarkymą, kurį vykdo Europos Sąjungos valstybių narių diplomatinės ar konsulinės įstaigos, veikiančios trečiųjų šalių teritorijoje. Tai gali būti ambasada ar konsulatas, laivas arba lėktuvas, kuriems pagal tarptautinę viešąją teisę ar tarptautinius susitarimus yra nustatyta Europos Sąjungos valstybės narės teisė[91]. Šios įstaigos yra laikomos duomenų valdytojais ar duomenų tvarkytojais ir joms, lygiai taip pat, turi būti taikomos Bendrojo duomenų apsaugos reglamento nuostatos.

2.4. Duomenų subjektų teisės bei jų įgyvendinimas

Kaip jau buvo minėta, Bendruoju duomenų apsaugos reglamentu yra išplečiamos bei įtvirtinamos visiškai naujos duomenų subjekto teisės. Pagrindinė priežastis, lėmusi šių teisių išplėtimą, buvo siekis sustiprinti duomenų subjekto galimybes kontroliuoti savo asmens duomenis. Dėl sparčiai besiplėsiančios skaitmeninės rinkos ir naujųjų technologijų sudėtingumo, duomenų subjektui sunku suvokti ir pastebėti, ar jo asmens duomenys renkami, kas juos renka ir kokiu tikslu, kaip antai reklama internete (Bendrojo duomenų apsaugos reglamento 58 p.). Atsižvelgus į tai, Bendruoju duomenų apsaugos reglamentu siekiama palengvinti duomenų subjekto naudojimąsi savo teisėmis, įskaitant mechanizmus, kaip prašyti ir atitinkamais atvejais visų pirma nemokamai gauti galimybę susipažinti su savo asmens duomenimis ir juos ištaisyti ar ištrinti bei pasinaudoti teise nesutikti su asmens duomenų tvarkymu.

Viena iš naujų teisių, kurias įgyja duomenų subjektas yra teisė į duomenų perkeliamumą. Bendrajame duomenų apsaugos reglamente numatyta, kad duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui

[91] ES 29 str. duomenų apsaugos darbo grupė. *2010 m. Nuomonė Nr. 8/2010 dėl taikytinos teisės* (WP 179), p. 15.

susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, ir teisę persiųsti tuos duomenis kitam duomenų valdytojui, o duomenų valdytojas, kuriam asmens duomenys buvo pateikti, turi nesudaryti tam kliūčių[92]. Atsižvelgus į tai, duomenų subjektas turi teisę ne tik gauti duomenis, juos saugoti asmeniniame įrenginyje ir naudoti savo asmeninėms reikmėms, bet ir persiųsti šiuos duomenis kitam paslaugų teikėjui be jokių kliūčių. Duomenų subjektas, taip pat, gali reikalauti, kad vienas duomenų valdytojas jo asmens duomenis tiesiogiai persiųstų kitam duomenų valdytojui, kai tai techniškai įmanoma. Tačiau ši teisė nėra absoliuti.

Atkreiptinas dėmesys, jog duomenų subjekto teisė į duomenų perkeliamumą gali būti įgyvendinta, kai asmens duomenys tvarkomi sutikimo pagrindu arba vykdant sutartį, kurios šalis yra duomenų subjektas, ir tik tada, kai tokie duomenys tvarkomi automatizuotomis priemonėmis. Ši teisė netaikoma, jeigu duomenų tvarkymas grindžiamas kitu teisiniu pagrindu, pavyzdžiui: teisėtais duomenų valdytojo interesais ar kita teisine prievole. Duomenų subjektai, taip pat neturėtų naudotis teise į perkeliamumą, jei duomenų valdytojas tvarko duomenų subjekto asmens duomenis, vykdydamas savo viešąsias pareigas (Bendrojo duomenų apsaugos reglamento preambulės 65 p.). Dar daugiau, teisė į perkeliamumą galioja tik tiems asmens duomenims, kurie yra susiję su šią teisę įgyvendinančiu duomenų subjektu ir, tik tokie, kurie yra pateikti duomenų valdytojui paties duomenų subjekto.

Duomenų perkeliamumu ne tik sustiprinamos duomenų subjektų teisės ir galimybė kontroliuoti su jais susijusius asmens duomenis, tačiau ir suteikiama galimybė perbalansuoti duomenų subjektų ir duomenų valdytojų santykį.[93] Tuo pačiu, užtikrinamas laisvas asmens duomenų judėjimas Europos Sąjungoje, o tai yra vienas pagrindinių Bendrojo duomenų apsaugos reglamento tikslų.

[92] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.
[93] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. Gairės dėl duomenų perkeliamumo*, WP 242 rev.01, 16/LT, p. 3.

Duomenų subjektams, taip pat, įtvirtinama teisė reikalauti ištrinti asmens duomenis („teisė būti pamirštam“). Kitaip tariant, ši teisė numato, jog Bendrajame duomenų apsaugos reglamente nustatytais atvejais duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius duomenis, o duomenų valdytojas yra įpareigotas tai padaryti. Pateikiami keli pavyzdžiai, kuomet ši teisė gali būti įgyvendinama: kai asmens duomenys nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi; kai duomenų subjektas atšaukė savo sutikimą, tvarkyti jo asmens duomenis; kai asmens duomenys buvo tvarkomi neteisėtai ir pan. Pabrėžtina, jog ši teisė nėra absoliuti ir gali būti ribojama. Atkreiptinas dėmesys, jog duomenų subjektas gali reikalauti, kad jo asmeniai duomenys būtų pašalinti ne tik Europos Sąjungoje, bet ir už jos ribų įsisteigusių duomenų valdytojų, kurie vykdo veiklą Europos Sąjungos teritorijoje ir tvarko jo asmens duomenis.

Dar viena naujovė Europos Sąjungos asmens duomenų apsaugos teisėje – tai Bendrajame duomenų apsaugos reglamente įtvirtinta duomenų subjekto teisė apriboti jo asmens duomenų tvarkymą. Duomenų tvarkymo apribojimas reiškia saugomų asmens duomenų žymėjimą siekiant apriboti jų tvarkymą ateityje[94]. Tokiu atveju, asmens duomenys, kurių tvarkymas yra apribotas, gali būti tik saugomi ir su tokiais duomenimis negali būti atliekami jokie kiti duomenų tvarkymo veiksmai. Minėta teisė yra prevencinė priemonė, kuria siekiama apsaugoti duomenų subjektą nuo gresiančių pavojų jo teisėms bei teisėtiems interesams.

Svarbu paminėti ir kitas, ne ką mažiau svarbias duomenų subjekto teises, kurios buvo perkeltos iš Duomenų apsaugos direktyvos į Bendrąjį duomenų apsaugos reglamentą. Viena tokių – teisė būti informuotam apie duomenų tvarkymą. Pagal šią teisę, duomenų subjektas privalo būti informuotas apie jo duomenų tvarkymą, o duomenų valdytojas turi pareigą pateikti

[94] *Ibid*., 4 str. 3 p.

tokią informaciją duomenų subjektui[95]. Pareiga pateikti informaciją apie asmens duomenų tvarkymą reiškia, jog duomenų valdytojas turi imtis aktyvių veiksmų, kad pasidalintų konkrečia informacija su duomenų subjektu ir jam pačiam nereikėtų ieškoti informacijos apie tokį duomenų rinkimą[96]. Pabrėžtina, jog ši informacija privalo būti pateikta glausta, skaidria ir duomenų subjektui suprantama forma. Ši duomenų subjekto teisė ir duomenų valdytojo pareiga kyla iš sąžiningo ir skaidraus duomenų tvarkymo principo. Bendrajame duomenų apsaugo reglamente nustatyta, kokia informacija privalo būti pateikta duomenų subjektams, nepriklausomai nuo duomenų tvarkymo ypatumų.

Visų pirma, duomenų subjektui turi būti nurodytas duomenų tvarkymo teisinis pagrindas bei duomenų tvarkymo tikslai, kurių siekiant ir bus tvarkomi jo asmens duomenys. Be kita ko, duomenų subjektui turi būti suteikiama informacija apie asmens duomenų saugojimo laikotarpį bei technines priemones, kuriomis duomenų valdytojas užtikrins tokią asmens duomenų apsaugą. Duomenų subjektas, taip pat, privalo būti informuotas apie savo teises, kurios jam suteiktos pagal Bendrąjį duomenų apsaugos reglamentą, įskaitant teisę pateikti skundą priežiūros institucijai.[97] Ši informacija laikoma bendrąja ir duomenų valdytojas ją privalo suteikti duomenų subjektui visais atvejais.

Pabrėžtina, jog, kai duomenis tvarko ne Europos Sąjungoje įsisteigusio duomenų valdytojo atstovas, duomenų subjektui turi būti pateikta informacija ne tik apie duomenų valdytojo, bet ir apie jo atstovo tapatybę bei kontaktinius duomenis. Nepaisant to, ši teisė nėra absoliuti ir gali būti apribota Europos Sąjungos arba nacionalinėje teisėje numatytais atvejais, arba kai siekiama apginti svarbesnius interesus. Svarbu paminėti, jog duomenų valdytojas privalo suteikti informaciją apie asmens duomenų tvarkymą per pagrįstą laikotarpį, tačiau ne

[95] *Ibid.,* 13 str. 1 d.
[96] ES 29 str. duomenų apsaugos darbo grupė. *Gairės dėl skaidrumo pagal Reglamentą* 2016/679, Nr. WP 260,p. 4.

vėliau kaip per 30 dienų[98]. Įgyvendinant šią teisę, užtikrinamas daug skaidresnis bei sąžiningesnis asmens duomenų tvarkymas.

Į Bendrąjį duomenų apsaugos reglamentą, taip pat, perkelta bei išplėsta duomenų subjekto teisė susipažinti su asmens duomenimis bei juos ištaisyti. Pagal šią teisę, duomenų subjektas gali reikalauti iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi – teisę susipažinti su asmens duomenimis ir gauti informaciją apie jų tvarkymą. Atsižvelgus į tai, duomenų subjektas turi teisę gauti tvarkomų asmens duomenų kopiją ar bet kokią kitą papildomą informaciją, susijusią su jo asmens duomenų tvarkymu.

Atkreiptinas dėmesys, kad su šia teise yra glaudžiai susijusi ir teisė reikalauti ištaisyti asmens duomenis. Duomenų subjektas, įgyvendindamas teisę susipažinti su asmens duomenimis, gali pastebėti, jog duomenų valdytojas tvarko netikslius ar pasenusius asmens duomenis. Tokiu atveju, duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas papildytų neišsamius asmens duomenis bei teisę reikalauti, kad duomenų valdytojas, nedelsdamas, ištaisytų netikslius asmens duomenis, pateikiant papildomą pareiškimą, Minėtos duomenų subjekto teisės užtikrina ir detalizuoja skaidrumo bei tikslumo principus.

Atsižvelgus į tai, kas išdėstyta, galima teigti, jog Bendrasis duomenų apsaugos reglamentas sustiprina duomenų subjektų teisių institutą, perkeldamas ir išplėsdamas tam tikras teises iš Duomenų apsaugos direktyvos bei įtvirtindamas visiškai naujas duomenų subjektų teises. Minėtų teisių įtvirtinimas padeda užtikrinti, kad asmens duomenys būtų pakankami, teisingi, naudojami tik teisėtais tikslais ir tik tų duomenų valdytojų, kurie turi teisę tokius duomenis tvarkyti. Taip siekiama įgyti didesnį duomenų subjektų pasitikėjimą Europos

[98] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.

Sąjungoje nustatyta duomenų apsaugos teisės sistema ir skatinti verslo plėtrą bei Europos Sąjungos valstybių narių globalizaciją.

3. ES BENDROJO DUOMENŲ APSAUGOS REGLAMENTO ĮTAKA KETVIRTOSIOS PRAMONĖS REVOLIUCIJOS TECHNOLOGIJŲ PLĖTRAI

Šiandieninis pasaulis tampa vis labiau skaitmeninis. Tai neišvengiama ketvirtosios pramonės revoliucijos pasekmė. Pabrėžtina, kad ketvirtosios pramonės revoliucijos technologijos yra neatsiejamai susijusios su kiekvieną dieną augančiu duomenų kiekiu. Naujosios technologijos leidžia iš duomenų sukurti daugybę įvairių fizinių objektų, atlikti veiksmus, teikti paslaugas[99]. Dar daugiau, duomenys yra reikalingi šių technologijų veikimui bei tolimesnei pažangai užtikrinti, įskaitant dirbtinio intelekto treniravimą, didžiųjų duomenų analizę, daiktų internetą ir kt. Ketvirtosios pramonės revoliucijos technologijos aktyviai prisideda prie kiekvieną dieną sukuriamo milžiniško duomenų kiekio, o tuo pačiu palieka elektroninius pėdsakus, kuriuose gausu ir asmeninės informacijos. Šios technologijos leidžia inovatyviais būdais rinkti, naudoti ir saugoti daugybę įvairiausių tipų asmens duomenų[100], todėl patenka į Bendrojo duomenų apsaugos reglamento taikymo sritį. Atsižvelgus į tai, šiame skyriuje bus aptartos pagrindinės ketvirtosios pramonės revoliucijos technologijos, įskaitant didžiuosius duomenis, dirbtinį intelektą, „blockchain“ technologiją ir daiktų internetą. Pasak tyrimų, šios technologijos laikomos kaip didžiausią potencialą turinčios technologijos, kurios lems reikšmingiausius pasikeitimus daugelyje visuomenei svarbių gyvenimo sričių[101]. Taip pat, bus analizuojamas šių technologijų ryšys su Bendruoju duomenų apsaugos reglamentu, jo reikšmė bei įtaka tolimesnei ketvirtosios pramonės revoliucijos technologijų pažangai.

[99] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 318.
[100] *Ibid*., p. 321.
[101] Information Systems Audit and Control Association. Digital Transformation Barometer (DTB). Research report, 2018. [interaktyvus, žiūrėta 2020m. kovo 29 d.]. Prieiga per internetą: https://www.isaca.org/-/media/info/digital-transformation-barometer/index.html

3.1. Bendrasis duomenų apsaugos reglamentas ir didieji duomenys

Kiekvieną dieną pasaulyje sugeneruojamų duomenų kiekis sparčiai didėja – nuo 33 zetabaitų 2018 m. iki numatomų 175 zetabaitų 2025 m[102]. Sparčiai vystantis naujoms technologijoms, atsiranda vis daugiau naujų duomenų rūšių, kuriuos per sudėtinga apdoroti naudojant tradicines priemones bei metodus. Dėl šios priežasties, pradėta vartoti nauja sąvoka „didieji duomenys“.

„Didieji duomenys“ (angl. *big data*) - apibūdinami kaip pažangių skaitmeninių technologijų pagalba renkamas, analizuojamas bei apdorojamas ypatingai didelis kiekis duomenų, kurių negalima apdoroti naudojant tradicines priemones ir analizės metodus. Kitaip tariant, tai - žmonių ar mašinų generuojami milžiniški duomenų masyvai, pasižymintys didele apimtimi, sparta bei įvairove. Didžiųjų duomenų naudojimas veda link duomenimis paremtos visuomenės formavimo, kadangi tokie duomenys apima vis daugiau asmens gyvenimo aspektų[103]. Didžiųjų duomenų analizė labai dažnai apima ir asmeninę informaciją. Sparčiai vystantis skaitmeninėms technologijoms, atsiranda vis daugiau skirtingų duomenų rūšių, galinčių identifikuoti duomenų subjektą. Anksčiau duomenų subjekto tapatybė galėjo būti nustatyta tik pagal standartinius asmens duomenis, tokius kaip: vardas ir pavardė, adresas, socialinio draudimo numeris. Šiandieniniame pasaulyje duomenų subjektai gali būti identifikuoti ir pagal buvimo vietą, savo pirkimo įpročius ar net socialiniuose tinkle išreikštus pomėgius.

Naudojant didžiųjų duomenų analizę, verslo subjektai gali pasiūlyti vartotojams suasmenintus prekių bei paslaugų pasiūlymus, kurie labiausiai atitiktų vartotojų poreikius. Tuo

[102] 2018 m. IDC atliktas tyrimas dėl duomenų kiekio [interaktyvus, žiūrėta 2020 m. kovo 28 d.]. Prieiga per internetą:https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
[103] MAYER-SCHONBERG, V; CUKIER, K. Big Data: A Revolution That Will Transform How We Live, Work and Think, *London: John Murray*, 2013, p. 73.

tarpu, paieškos sistemos analizuoja vartotojų užklausas tam, kad pateiktų kuo tikslesnius paieškos rezultatus. Pavyzdžiui, interneto gigantas „Google“ renka duomenis, kad galėtų tobulinti savo paieškos algoritmus ir plėtoti naujas išsamias duomenų rinkimo paslaugas, tokias kaip balso atpažinimas, teksto vertimas ar padėties nustatymas[104]. Tinkamai panaudoti, didieji duomenys skatina inovacijas verslo ir technologijų srityje, veda prie efektyvesnio rizikos valdymo. Taip pat pasitarnauja sveikatos priežiūros srityje, atliekant įvairius tyrimus, pagal kuriuos daug tiksliau vertinamas vaistų ar tam tikrų gydymo metodų veiksmingumas. Nepaisant to, didžiųjų duomenų analizė suteikia tiek pat galimybių, kiek gali sukelti potencialios žalos duomenų subjektams, kurių asmens duomenys yra tvarkomi bei analizuojami, taip pat kitiems asmenims, kuriems tokia duomenų analizė daro netiesioginį poveikį[105].

Vienas iš pavojų, susijusių su didžiųjų duomenų analize, yra asmens duomenų kontrolės stoka bei netinkamas skaidrumo principo įgyvendinimas. Bendrajame duomenų apsaugos reglamento 5 straipsnio 1 dalies b punkte įtvirtintas skaidrumo principas, pagal kurį fiziniams asmenims turi būti suteikiama informacija, kaip su jais susiję asmens duomenys yra renkami, naudojami, taip pat kokiu mastu tie asmens duomenys yra ar bus tvarkomi (Bendrojo duomenų apsaugos reglamento preambulės 39 p.). Bendrojo duomenų apsaugos reglamento 13 bei 14 straipsniuose numatyta duomenų subjekto teisė susipažinti su asmens duomenimis bei duomenų valdytojo pareiga informuoti duomenų subjektą apie asmens duomenų tvarkymą. Šiomis nuostatomis konkrečiai įgyvendinamas minėtas skaidrumo principas. Atsižvelgus į tai, asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais, o

[104] RUBINSTEIN, S. Ira. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, 2013, Vol. 3, No. 2, p. 3.
[105] ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017, p. 995.

tolesnis duomenų tvarkymas su tais tikslais nesuderinamu būdu yra draudžiamas[106]. Deja, didžiųjų duomenų analizavimas dažnai apima tokius metodus ir duomenų naudojimo būdus, kurių duomenų rinkimo metu nei duomenų subjektas, nei duomenų valdytojas neaptarė ar net neįsivaizdavo[107]. Dėl šios priežasties, nėra tinkamai užtikrinamas skaidrumo principas, kadangi, daugeliu atvejų, duomenų subjektas net nežino apie savo asmens duomenų tvarkymą arba negali atsekti, kaip tokie duomenys perduodami iš vieno šaltinio į kitą. Taip pat, duomenų subjektai gali netekti galimybės naudotis savo teisėmis ir jiems užkertamas kelias kontroliuoti savo asmens duomenis.

Pabrėžtina, jog daugeliu atvejų, atliekant didžiųjų duomenų analizę, iš duomenų, kurie nėra laikomi asmens duomenimis, sujungtų su kitais duomenų rinkiniais, yra išvedama nauja informacija, galinti identifikuoti asmenį ar asmenų grupę[108]. Taigi, tvarkomų asmens duomenų kiekis laikui bėgant gali keistis. Atsižvelgus į tai, kyla abejonių ar duomenų valdytojas turi galimybę bet kuriuo metu suteikti tikslią informaciją duomenų subjektui apie jo tvarkomus asmens duomenis, kaip to reikalauja Bendrasis duomenų apsaugos reglamentas.

Grėsmė asmens duomenų apsaugai kyla ir dėl pakartotinio duomenų subjekto identifikavimo. Bendrajame duomenų apsaugos reglamente numatyta, jog anonimiškai informacijai, t. y. informacijai, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta, šis reglamentas yra netaikomas (Bendrojo duomenų apsaugos reglamento preambulės 27 p.). Nepaisant to, didžiųjų duomenų analizė, naudojanti anonimiškus duomenis, leidžia pakartotinai nustatyti duomenų subjekto tapatybę, todėl kyla daugelis klausimų dėl esminio skirtumo tarp asmens

[106] ES 29 str. duomenų apsaugos darbo grupė. *2017 m. Skaidrumo užtikrinimo pagal Reglamentą (ES) 2016/679 gairės*. WP260, 1 red. 17/LT, p. 25.
[107] ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017, p. 997.
[108] RUBINSTEIN, S. Ira. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, 2013, Vol. 3, No. 2, p. 4.

duomenų ir anonimiškų duomenų[109]. Pakartotinis duomenų subjekto tapatybės nustatymas gali rimtai paveikti asmenų privatumą. Vienas tokių pavyzdžių, mažmeninė prekybos bendrovė „Target“, kuri išanalizavusi savo klientų pirkimo istoriją ir internetines paieškas, identifikavo klientes bei nustatė, kurios iš jų šiuo metu yra nėščios[110]. Šioms klientėms buvo išsiųsti nuolaidų kuponai, skirti kūdikių prekėms. Labiausiai stebina tai, jog kai kurios iš jų dar nebuvo atskleidę nėštumo fakto net savo artimiesiems.

Kalbant apie didžiųjų duomenų analizę, svarbu paminėti ir tikslo apribojimo principą. Kaip jau minėta, pagal šį principą asmens duomenys turi būti renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu[111]. Nepaisant to, daugeliu atveju, surinkti asmens duomenys taip pat gali būti tikrai naudingi ir kitiems tikslams, kurie iš pradžių nebuvo nurodyti[112]. Tuo labai dažnai pasižymi profiliavimas. Bendrojo duomenų apsaugos reglamento 4 straipsnio 4 dalyje profiliavimas apibrėžtas kaip „bet kokios formos automatizuotas asmens duomenų tvarkymas, kurį vykdant vertinami su fiziniu asmeniu susiję asmeniniai aspektai, visų pirma siekiant analizuoti arba numatyti aspektus, susijusius su duomenų subjekto darbo rezultatais, ekonomine padėtimi, sveikatos būkle, asmeniniais pomėgiais ar interesais, patikimumu arba elgesiu, vieta arba judėjimu, kai tai jo atžvilgiu sukelia teisinių pasekmių arba jam daro panašų didelį poveikį“. Pažymėtina, jog tokio pobūdžio asmens duomenų tvarkymas apima gana platų duomenų subjektų stebėjimo veiklos spektrą, pavyzdžiui: individualizuotos dietos ir sveikatos analizės paslaugas internete, vaizdo stebėjimo sistemas (CCTV), rinkodaros tikslais vykdomus tyrimus, duomenų subjektų

[109] OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 2010, 57 *UCLA Law Review* 1701, University of Colorado Law Legal Studies Research Paper No. 9-12, p. 45.
[110] Forbes. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did* [interaktyvus, žiūrėta 2020 m. kovo 28 d.]. Prieiga per internetą: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2ff78d2f6668.
[111] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.
[112] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė Nr. 03/2013 dėl tikslo ribojimo*. 00569/13/EN, WP 203, p. 4.

sveikatos būklės stebėjimą ir t.t. Atkreiptinas dėmesys, kad, naudojant profiliavimą, dažnai yra tvarkomi ir specialiųjų kategorijų asmens duomenys, kurių tvarkymui yra taikomi itin griežti reikalavimai.

Duomenų analizės tyrimai rodo, jog daugelis žmonių asmeninių savybių, pradedant seksualine orientacija bei politinėmis pažiūromis ir baigiant socialine padėtimi ar net intelektu, gali būti tiksliai nustatomos pagal „Patinka“ paspaudimus socialiniame tinkle „Facebook“[113]. Atsižvelgus į tai, kyla klausimas: ar profiliavimas visuomet yra tikslinga ir etiška veikla? Į šį klausimą geriau atsakyti padės pateikti pavyzdžiai. Londone įsikūrusi tyrimų bendrovė „Cambridge Analytica“, 2016 m. JAV prezidento rinkimuose neteisėtai panaudojo daugiau nei 50 mln. „Facebook“ vartotojų asmens duomenis, kad siųstų jiems tikslinę politinę reklamą, kuri galėjo paveikti šių asmenų pasirinkimą[114]. Tuo tarpu dauguma Jungtinėje Karalystėje veikiančių labdaros organizacijų ilgą laiką rinko bei kaupė asmeninę esamų ir buvusių aukotojų informaciją, paremtą turto patikra (ang. *wealth screening*). Pavyzdžiui, labdaros organizacija „Cancer Research“ profiliavo 3,5 mln. aukotojų, suklasifikavo juos pagal jų turimą turtą, ir atsekė beveik 700 tūkst. telefono numerių, siekdami jiems išsiųsti rinkodaros pranešimus. Negana to, kai kurios labdaros organizacijos prekiavo aukotojų asmenine informacija su kitomis labdaros organizacijomis[115]. Atsižvelgus į minėtus pavyzdžius, galima teigti, jog asmens duomenų tvarkymas, įskaitant profiliavimą, dažnai apima ir tokius asmens duomenų tvarkymo tikslus, kurie iš pradžių nebuvo tinkamai nurodyti arba išvis nėra suderinami su pirminiais duomenų tvarkymo tikslais. Tokiu būdu yra pažeidžiamas tikslo apribojimo

[113] KOSINSKIA, Michal; STILLWELLA, David; GRAEPELB, Thore. *Private traits and attributes are predictable from digital records of human behavior* [interaktyvus, žiūrėta 2020 kovo 10 d.]. Prieiga per internetą: https://www.pnas.org/content/pnas/110/15/5802.full.pdf .

[114] *The Guardian.* Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach [interaktyvus, žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[115] *The Guardian. UK charities fined by watchdog for wealth screening of donors* [interaktyvus, žiūrėta 2020 m. kovo 12 d.]. Prieiga per internetą: https://www.theguardian.com/uk-news/2017/apr/05/uk-charities-fined-by-watchdog-for-wealth-screening-of-donors.

principas. Atitinkamai, minėtas asmens duomenų tvarkymas gali sukelti neigiamus padarinius duomenų subjektams.

Apibendrinant, galima teigti, jog atliekant didžiųjų duomenų analizę, susiduriama su rimtomis grėsmėmis asmens duomenų apsaugai. Dėl šios priežasties, kaip niekad svarbu tinkamai interpretuoti bei taikyti Bendrąjį duomenų apsaugos reglamentą, siekiant užtikrinti veiksmingą duomenų subjektų teisių apsaugą.

3.2. Bendrasis duomenų apsaugos reglamentas ir dirbtinis intelektas

Vieningo atsakymo į klausimą, kas yra dirbtinis intelektas, nėra. Daugelis mokslininkų pateikia skirtingas dirbtinio intelekto sąvokas, todėl egzistuoja daug apibrėžimų. Tarptautiniuose terminų žodynuose dirbtinis intelektas apibrėžiamas kaip kompiuterinių sistemų, galinčių atlikti įvairias užduotis, kurioms paprastai reikalingas žmogaus intelektas, tobulinimas bei plėtra, pavyzdžiui: kalbos atpažinimas, automatinių sprendimų priėmimas, kalbų vertimas[116] arba kaip mokslas, kaip sukurti mašinas, turinčias tam tikras žmogaus proto savybes, tokias kaip galimybę suprasti kalbą, atpažinti nuotraukas, spręsti problemas ir mokytis[117]. Tuo tarpu Europos komisija apibrėžia dirbtinį intelektą kaip sistemas, kurios demonstruoja protingą ir sumanų elgesį, analizuodamos savo aplinką ir darydamos gana savarankiškus sprendimus tikslui pasiekti[118]. Apibendrinant, dirbtinis intelektas suvokiamas kaip mašinų gebėjimas teisingai interpretuoti duomenis, mokytis iš jų ir panaudoti sukauptas žinias, siekiant įgyvendinti konkrečius tikslus bei atlikti intelekto reikalaujančias užduotis. Didžiausias dirbtinio intelekto skirtumas nuo kitų programų ar panašių robotų yra tai, jog atlikdamas tą patį veiksmą daugelį kartų, jis gali išanalizuoti jau atliktus veiksmus, pats save

[116] The Oxford Dictionary of Phrase and fable, Second Edition. *Oxford University Press*, 2006, p. 134.
[117] Cambridge Advanced Learner's Dictionary. Third Edition. *Cambridge University Press*, 2008, p. 751.
[118] 2018 m. balandžio 24 d. Komisijos Komunikatas Europos Parlamentui, Europos Vadovų Tarybai, Europos Tarybai, Europos Ekonomikos ir Socialinių reikalų komitetui ir Regionų komitetui. *Dirbtinis intelektas Europai*. COM/2018/237 final, p. 16.

mokyti ir elgtis kitaip, jei tai padeda efektyviau pasiekti nurodytus tikslus bei uždavinius. Atsižvelgus į tai, programa, naudojanti dirbtinį intelektą, palaipsniui tampa „protingesnė“. Tokiu pačiu principu pagrįstas ir mašininis mokymasis (ang. *machine learning*), kuris, naudodamas algoritmus, renka, analizuoja bei apdoroja duomenis iš realaus pasaulio. Šia technologija siekiama pateikti vartotojui kuo geresnius bei tikslesnius rezultatus.

Dirbtinio intelekto galimybės ypač sparčiai vystėsi pastaraisiais metais. Dirbtinis intelektas, apdorodamas didžiulius duomenų kiekius, kad būtų galima pasiūlyti veiksmingus sprendimus, prisideda prie produktų, procesų ir verslo modelių tobulinimo visuose ekonomikos sektoriuose.[119] Šiuo metu jis taikomas įvairiuose sektoriuose: tiek viešajame, tiek privačiame sektoriuose. Pradedant nuo programų, kurios verčia dokumentus, filtruoja el. laiškus, atpažįsta veidus ir balsus, baigiant lėtinių ligų gydymu, mirtingumo mažinimu eismo įvykiuose, kova su klimato kaita ar kibernetinio saugumo užtikrinimu[120]. Atkreiptinas dėmesys, jog dirbtinį intelektą ir didžiuosius duomenis sieja abipusis ryšys: dirbtinis intelektas naudoja bei analizuoja duomenis, siekdamas kuo tiksliau atlikti intelekto reikalaujančias užduotis bei įvykdyti nurodytus tikslus, o dirbtinio intelekto pagalba, didieji duomenys yra daug lengviau renkami bei apdorojami. Kitaip tariant, duomenys yra dirbtinio intelekto „variklis“, nes be jų, dirbtinis intelektas negali tobulėti ir išnaudoti viso savo potencialo. Dirbtinis intelektas bei mašininio mokymosi metodai dažnai naudojami tvarkant asmens duomenis, pavyzdžiui: atliekant studentų duomenų iš virtualios mokymosi aplinkos analizę, kuria siekiama tobulinti mokymo medžiagą arba renkant viešojo transporto keleivių maršrutų duomenis, siekiant pagerinti viešojo transporto teikiamas paslaugas[121]. Atsižvelgus į minėtus pavyzdžius,

[119] 2018 m. gruodžio 7 d. Komisijos Komunikatas Europos Parlamenti, Europos Vadovų Tarybai, Europos Tarybai, Europos Ekonomikos ir Socialinių reikalų komitetui ir Regionų komitetui. *Suderintas dirbtinio intelekto planas* COM(2018) 795, p. 1.
[120] KUNER, Christopher; CATE H. Fred; MILLARD, Christopher. et.al. Expanding the artificial intelligence-data protection debate. *International Data Privacy Law*, 2018, Vol. 8, No. 4, p. 289.
[121] BUTTERWORTH, Michael. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2018, p. 2.

netinkamas ar neteisėtas asmens duomenų tvarkymas, naudojant dirbtinį intelektą, gali sukelti itin neigiamas pasekmes duomenų subjektams.

Didžiausias iššūkis su kuriuo susiduriama naudojant dirbtinį intelektą, yra tinkamas duomenų subjektų teisių, susijusių su automatiniu sprendimų vykdymu, įgyvendinimas. Kaip jau buvo minėta, Bendrojo duomenų apsaugos reglamento 15 straipsnyje numatyta duomenų subjekto teisė susipažinti su duomenimis, pagal kurią „duomenų subjektas turi teisę reikalauti iš duomenų valdytojo pateikti informaciją apie loginį automatinio sprendimų vykdymo proceso pagrindimą, taip pat tokio duomenų tvarkymo reikšmę ir numatomas pasekmes duomenų subjektui“[122]. Svarbu pabrėžti, kad dirbtinis intelektas yra paremtas automatiniu sprendimų vykdymo procesu, kuris apibūdinamas kaip gebėjimas priimti sprendimus techninėmis priemonėmis, nesikišant žmonėms. Automatizuoti sprendimai priimami, remiantis plataus masto asmens duomenimis, pavyzdžiui: susijusių asmenų tiesiogiai suteiktais duomenimis, stebint asmenis gautais duomenimis (programinės įrangos surinktais vietos nustatymo duomenimis); išvestiniais arba numanomais duomenimis (pvz.: sudarytu kredito reitingu)[123]. Tokiam procesui įgyvendinti naudojami itin sudėtingi algoritmai, kurie sugeba internalizuoti duomenis, todėl paaiškinti kaip jie veikia ar atsekti ir pateikti informaciją, kaip vienoks ar kitoks sprendimas buvo priimtas, dažnai gali būti per daug sudėtinga. Negana to, įmonėms tai gali kainuoti labai brangiai, kadangi tokiai informacijai pateikti reikalingas didelis kiekis žmogiškųjų išteklių. Tuo tarpu dirbtinio intelekto atmainų, tokių kaip gilusis mokymas (ang. *deep learning*) veikimo neįmanoma paaiškinti žmonėms suprantamu būdu, kadangi jis yra paremtas neuroninio tinklo[124] (angl. *neural network*) pagrindu. Dėl šios priežasties, dirbtinis

[122] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.
[123]ES 29 str. duomenų apsaugos darbo grupė. *Automatizuoto atskirų sprendimų priėmimo ir profiliavimo pagal Reglamentą 2016/679 gairės,* 17/LT WP251, 1 red., p. 8.
[124] Neuroninis tinklas - tinklas, atkartojantis neuronų tinklo savybes ir veikiantis panašiu principu, kaip ir smegenys.

intelektas dažnai vadinamas „juodąja dėže“[125]. Atsižvelgus į tai, gali būti itin sudėtinga tinkamai įgyvendinti duomenų subjekto teisę susipažinti su duomenimis.

Atkreiptinas dėmesys, kad Bendrojo duomenų apsaugos reglamento 22 straipsnio 1 dalyje įtvirtinta duomenų subjekto teisė, pagal kurią jis gali pasirinkti „kad jam nebūtų taikomas tik automatizuotu duomenų tvarkymu, įskaitant profiliavimą, grindžiamas sprendimas, dėl kurio jam kyla teisinės pasekmės arba kuris jam panašiu būdu daro didelį poveikį.“ Dar daugiau, šio teisės akto 17 straipsnio 1 dalyje numatyta duomenų subjekto teisė reikalauti ištrinti asmens duomenis („teisė būti pamirštam“). Kaip jau minėta, dirbtinio intelekto veikimui bei tobulėjimui, reikalingi milžiniški duomenų kiekiai, kurių didelę dalį užima ir asmens duomenys. Dėl šios priežasties, minėtų duomenų subjekto teisių, numatytų Bendrajame duomenų apsaugos reglamente, įgyvendinimas gali sumažinti algoritmų, kuriais paremtas automatinių sprendimų vykdymas, efektyvumą bei tikslumą arba visiškai juos sunaikinti. Tokiu būdu gali būti ne tik apribojamas dirbtinio intelekto naudojimas, bet ir užkertamas kelias tolimesnei dirbtinio intelekto pažangai[126].

Apibendrinant, galima teigti, jog Bendrasis duomenų apsaugos reglamentas neišvengiamai įtakoja dirbtinio intelekto bei mašininio mokymosi plėtrą bei tolimesnį naudojimą praktikoje.

3.3. Bendrasis duomenų apsaugos reglamentas ir daiktų internetas

Viena iš greičiausiai besivystančių ir didžiausią potencialą turinčių ketvirtosios pramonės revoliucijos technologijų inovacijų yra daiktų internetas. Paprastai tariant, daiktų internetas (angl. *Internet of Things*) – tai nauja tinklų konfigūracija, apimanti fizinių objektų

[125] BATHAEE, Yavar. The Artificial Intelligence black box and the failure of intent and causation. *Harvard Journal of Law & Technology*, Volume 31, Number 2, 2018, p. 901.
[126] LI, He; YU, Lu; HE, Wu. The Impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, 2019, VOL. 22, NO. 1, p. 3.

komunikavimą ir objektų bei žmonių sąveiką internete[127]. Daiktų internetas laikomas nauja interneto evoliucijos pakopa, kurioje daiktai tampa aktyvūs verslo, informacijos ir socialinių procesų dalyviai, galintys komunikuoti ir sąveikauti tarpusavyje ir su išmaniąja aplinka keisdamiesi duomenimis, autonomiškai reaguoti į fizinio pasaulio įvykius bei veikti aplinką atliekant įvairius veiksmus ir teikiant paslaugas[128]. Artimiausiais metais numatomas milžiniškas šio sektoriaus augimas. Kaip jau buvo minėta, pasaulio lyderiai bei mokslininkai prognozuoja, kad 2020 m. prie interneto bus prijungta 50 mlrd. įrenginių[129], o tai lygu maždaug šešiems tarpusavyje sujungtiems išmaniems įrenginiams kiekvienam asmeniui pasaulyje.

Daiktų interneto technologija yra paremta plataus masto duomenų tvarkymu, o tokie duomenys dažniausiai susiję su fiziniais asmenimis, kurių tapatybė nustatyta arba gali būti nustatyta[130]. Atitinkamai, šie duomenys yra laikomi asmens duomenimis. Atsižvelgus į tai, daiktų interneto technologijai yra taikomas dabartinis asmens duomenų apsaugos teisinis reguliavimas, numatytas Bendrajame duomenų apsaugos reglamente. Tyrimai rodo, kad daiktų internetas suteikia įmonėms duomenis, kurių jiems reikia, norint pagerinti rinkodaros galimybes, didinant pardavimus ir sumažinant papildomas išlaidas. Prognozuojama, jog 2025 m. daiktų interneto ekonominis poveikis sieks 11 trilijonų dolerių[131].

---

[127] SAVUKYNAS, Raimundas; MARCINKEVIČIUS, Virginijus. Daiktų interneto objektų identifikavimo metodų palyginimas. *Informacijos mokslai*. 2017, Nr. 78, p. 67.

[128] GUBBI, J.; BUYYA, R.; MARUSIC, S.; PA- LANISWAMI, M. (2013). Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions. *Journal of Future Generation Computer Systems,* 29(7): 1645–1660.

[129] World Economic forum. Survey Report. *Global Agenda Council on the Future of Software & Society Deep Shift Technology Tipping Points and Societal Impact*, 2015, p. 16 [interaktyvus, žiūrėta 2020 m. kovo 30 d.]. Prieiga per internetą:http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.

[130] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.

[131] Mckinsey Global Institute. The Internet of Things: mapping the value beyond the hype. *Executive summary*, June 2015, p. 2 [interaktyvus, žiūrėta 2020 m. kovo 18 d.]. Prieiga per internetą: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.ashx.

Daiktų internetas gali pasitarnauti daugelyje sričių, pvz. pagerinti eismo saugumą, sveikatos būklę, sustiprinti apsaugą, padėti žmonėms taupyti energiją, pagreitinti pramoninius procesus ir t.t. Nepaisant visų šios technologijos teikiamų privalumų, daiktų interneto technologija kelia naujų iššūkių, susijusių su asmens duomenų apsauga.

Viena pagrindinių problemų, su kuria susiduriama, šioje srityje yra jau minėta asmens duomenų kontrolės stoka. Naudojant daiktų interneto technologiją, dažnais atvejais, duomenų subjektui gali būti itin sudėtinga kontroliuoti kaip tvarkomi jo asmens duomenys. Visų pirma, daugybė tarpusavyje sujungtų išmaniųjų įrenginių net neturi ekranų, o komunikacija su vartotojais vyksta pasitelkus šviesos, balso atpažinimo ar jutiklines technologijas, pavyzdžiui: įvairios apsaugos sistemos, išmaniosios kolonėlės, išmanioji stebėjimo įranga ir t.t. Dėl šios priežasties, duomenų subjektams gali būti sunku suprasti, kokie asmens duomenys apie juos yra renkami ir kaip jie yra panaudojami. Antra, duomenų subjektas taip pat gali neturėti galimybės tinkamai peržiūrėti daiktų internetu perduodamų duomenų, prieš juos paskelbiant, todėl neabejotinai kyla rizika, kad duomenų subjektas taip gali stokoti kontrolės ir paviešinti per daug informacijos apie save[132]. Trečia, išmanieji įrenginiai gali sąveikauti tarpusavyje be žmogaus įsikišimo ir automatiškai perduoti duomenis vieni kitiems, duomenų subjektui to net nežinant. Atsižvelgus į tai, laikui bėgant, gali būti nepaprastai sunku kontroliuoti renkamų asmens duomenų srautą bei tolesnį jų naudojimą, kuris gali įtakoti nepageidaujamą nukrypimą nuo išmanaus įrenginio funkcijų[133]. Dėl šios priežasties, gali susiklostyti situacija, kai duomenų subjektas visiškai nebekontroliuoja kokiu mastu yra renkami bei tvarkomi jo asmens duomenys, todėl negali tinkamai įgyvendinti savo teisių, numatytų Bendrajame duomenų apsaugos reglamente.

[132] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 8/2014 dėl pastarojo meto tendencijų, susijusių su daiktų internetu*, 2014, 1471/14/LT WP 223, p. 7.
[133] URQUHART, Lachlan; LODGE, Tom; CRABTREE, Andy. Demonstrably doing accountability in the Internet of Things. *International Journal of Law and Information Technology*, 2019, 27, 1–27, p. 4.

Kita problema, susijusi su daiktų internetu yra duomenų subjekto sutikimo kokybė. Kaip jau minėta, vienas iš svarbiausių asmens duomenų tvarkymo pagrindų, numatytų Bendrajame duomenų apsaugos reglamente yra duomenų subjekto sutikimas tvarkyti jo asmens duomenis. Sutikimas apibrėžiamas kaip „bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiškais veiksmais, kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys[134].“ Atitinkamai, tyla, iš anksto pažymėti langeliai arba neveikimas neturėtų būti laikomi sutikimu (Bendrojo duomenų apsaugos reglamento preambulės 32 p.). Nepaisant to, daugeliu atvejų, duomenų subjektas gali net nežinoti, kad tam tikri išmanieji įrenginiai tvarko jo asmens duomenis. Praktikoje projektuojami jutikliniai prietaisai dažniausiai patys neteikia informacijos ir juose nėra patikimų priemonių, kurias naudojant būtų galima gauti asmens sutikimą, kad duomenys būtų tvarkomi[135]. Pavyzdžiui, išmanieji laikrodžiai, kuriuose gali būti įtaisytų mikrofonų ar judesio jutiklių, renkančių ir perduodančių duomenis asmenims to nežinant ir juo labiau nedavus sutikimo, kad tokie asmens duomenys būtų tvarkomi[136], ar autonominiai automobiliai, kurie, turės galimybę dalintis tokiais asmens duomenimis, kaip buvimo vietos informacija ar kelionių istorija su kitomis transporto priemonėmis, techninės apžiūros paslaugas teikiančiu personalu ar transporto priemonės gamintoju be duomenų subjekto sutikimo[137]. Būtent dėl daiktų interneto technologijos sudėtingumo, gauti tikslaus duomenų subjekto sutikimo pagal Bendrajame duomenų apsaugos reglamente numatytus

[134] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016.
[135] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 8/2014 dėl pastarojo meto tendencijų, susijusių su daiktų internetu*, 2014, 1471/14/LT WP 223, p. 8.
[136] *Ibid*., p. 9.
[137] SURAKITBANHARN, Caitlin A., et. Al. Preliminary Ethical, Legal and Social Implications of Connected and Autonomous Transportation Vehicles (CATV). *Policy Research Institute, Purdue University* [interaktyvus, žiūrėta 2020 m. balandžio 6 d.]. Prieiga per internetą: https://www.purdue.edu/discoverypark/ppri/docs/Literature%20Review_CATV.pdf

reikalavimus, gali būti faktiškai neįmanoma arba toks sutikimas gali būti „nekokybiškas“ dėl duomenų valdytojo pateiktos informacijos stokos.

Kaip vieną iš iššūkių, susijusių su daiktų internetu, galima paminėti ir profiliavimą. Kaip jau minėta, daiktų interneto įrenginiai renka bei tvarko didelį kiekį asmens duomenų, o daugeliu atvejų jais dalinasi tarpusavyje be žmogaus įsikišimo. Net jeigu šie įrenginiai atskirai renka skirtingų rūšių informaciją apie asmenį, surinkus ir toliau analizuojant pakankamą duomenų kiekį tokių duomenų, iš jų galima sužinoti konkrečių dalykų apie asmens įpročius ar elgesio ypatumus[138]. Tokie asmenų stebėjimo bei profiliavimo metodai, pagrįsti susietais duomenimis, gali atskleisti itin jautrią informaciją apie duomenų subjektų tapatybę ir asmeninį gyvenimą, o tai gali privesti prie ekonominės, socialinės ir kitokio pobūdžio diskriminacijos[139]. Tokia diskriminacija

Atsižvelgus į tai, kas išdėstyta, galima teigti, jog pagrindiniai iššūkiai, su kuriais susiduriama asmens duomenų apsaugos srityje, taikant daiktų interneto technologiją, yra asmens duomenų kontrolės stoka, duomenų subjekto sutikimo kokybė bei duomenų subjektų diskriminaciją keliantis asmenų profiliavimas.

3.4. Bendrasis duomenų apsaugos reglamentas ir „Blockchain“ technologija

Blokų grandinė (ang. *Blockchain*) laikoma viena reikšmingiausių technologijų šiandieniniame pasaulyje. Oficialiai „Blockchain“ technologija apibrėžiama, kaip vieša decentralizuota sistema, skirta užfiksuoti bei saugoti tarp šalių įvykusias transakcijas[140]. Kitaip tariant, tai yra tam tikra duomenų bazė, kurioje saugoma visa informacija apie įvykusias transakcijas. Užfiksuotos transakcijos virsta skaitmeniniais įrašais, kurie vadinami „blokais“.

[138] *Ibid*, p. 9.
[139] WATCHER, Sandra. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 32 (2018), p. 437.
[140] KUNER, Christopher; CATE, Fred; LYNSKEY, Orla; , MILLARD, Christopher; LOIDEAIN, Ni Nora, SVANTESSON, Dan. Blockchain versus data protection. *International Data Privacy Law*, Volume 8, Issue 2, May 2018, p. 103.

Atitinkamai, tokie „blokai“ chronologine tvarka jungiasi vienas prie kito ir taip sudaro blokų grandinę. Šiandieniniame pasaulyje, tikriausiai įprasta, jog, vykdant virtualias transakcijas (siekiant atsiskaityti už prekes ir paslaugas ar pervesti pinigų), procese dalyvauja ir „tarpininkas“ – dažniausiai bankas ar kita elektroninių pinigų institucija. Tuo tarpu, „blockchain“ technologija leidžia asmenims kontaktuoti bei vykdyti tokias transakcijas tiesiogiai, be jokių trečiųjų šalių. Naudojant kriptografiją (informacijos užšifravimą ir dešifravimą), sukuriama skaitmeninė „buhalterinės apskaitos knyga“, kurioje esančias transakcijas gali matyti tik tie, kurie yra prisijungę prie tokios sistemos. Tačiau, kaip „blockchain“ technologija yra susijusi su asmens duomenimis? Tokiam paaiškinimui, būtina detaliau įsigilinti į tai, kaip veikia „blockchain“ technologija.

Pasitelkus kriptografijos metodą, tokia sistema užšifruoja įvykusių transakcijų duomenis, tarp kurių egzistuoja ir didelis kiekis asmens duomenų, todėl šiuos duomenis gali iššifruoti tik asmenys, turintys specialų priėjimą prie tokios informacijos, dar kitaip vadinamą „privačiu raktu“. Iš pirmo žvilgsnio gali pasirodyti, jog duomenys, kurie yra tvarkomi „blockchain“ sistemoje, yra anonimizuoti ir tokios informacijos neįmanoma tiesiogiai susieti su duomenų subjektu. Kaip jau minėta, pagal Bendrojo duomenų apsaugos reglamento 4 straipsnio 1 dalį, asmens duomenys reiškia „bet kokią informaciją, susijusią su fiziniu asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta“. Atkreiptinas dėmesys, kad prie asmens duomenų priskiriami ir IP adresai, kaip tai nustatė Europos Sąjungos Teisingumo Teismas byloje *Patrick Byer vs. Germany*[141]. Tačiau, atidžiau išanalizavus Bendrojo duomenų apsaugos reglamento teisinį reguliavimą, paaiškėja, jog didelis kiekis duomenų, kurie saugomi „blockchain“ sistemoje, yra laikomi asmens duomenimis, kadangi, pagal šiuos duomenis, gali būti nustatyta asmens tapatybė. Kitaip tariant, tokie duomenys nėra iki galo anonimizuoti,

[141] Europos Sąjungos Teisingumo Teismo 2016 m. spalio 19 d. sprendimas byloje C-582/14 Patrick Breyer v. Bundesrepublik Deutschland.

jiems tiesiog sukuriami pseudonimai. Remiantis Bendrojo duomenų apsaugos reglamento 26 konstatuojamąja dalimi: „asmens duomenimis, kuriems suteikiami pseudonimai ir kurie galėtų būti priskirti fiziniam asmeniui pasinaudojus papildoma informacija, turėtų būti laikomi informacija apie fizinį asmenį, kurio tapatybė gali būti nustatyta.“ Taigi, pakanka to, kad trečioji šalis sugebėtų identifikuoti asmenis pagal duomenis, naudojamus „blockchain“ technologijoje. Atsižvelgus į tai, duomenų kodavimas pseudonimais nėra laikomas duomenų nuasmeninimo metodu. Tai – tik galimybės duomenų rinkinį susieti su duomenų subjekto pirmine tapatybe sumažinimas, t. y. naudinga saugumo priemonė[142]. Dėl šios priežasties, pseudonimais užkoduotų duomenų negalima prilyginti nuasmenintai informacijai, nes, naudojantis tokiais duomenimis, išlieka galimybė išskirti pavienį duomenų subjektą ir jį susieti su įvairiais duomenų rinkiniais. Atsižvelgus į tai, „blockchain“ technologijos tvarkomi duomenys patenka į asmens duomenų apsaugos reguliavimo sritį ir šiems duomenims privalo būti taikomas Bendrasis duomenų apsaugos reglamentas.

Atitinkamai, dėl specifinio „blockchain“ technologijos pobūdžio, susiduriama su Bendrajame duomenų apsaugos reglamente numatytų reikalavimų įgyvendinimo probleminiais aspektais. Visų pirma, Bendrasis duomenų apsaugos reglamentas remiasi prielaida, kad kiekviename asmens duomenų tvarkymo etape, egzistuoja duomenų valdytojas, į kurį duomenų subjektai gali kreiptis siekdami įgyvendinti savo teises pagal dabartinį duomenų apsaugos teisinį reguliavimą[143]. Tačiau „blockchain“ technologijos pobūdis yra kitoks. Tai decentralizuota transakcijų fiksavimo sistema, kurios tvarkomi duomenys yra prieinami visiems, šia technologija besinaudojantiems, vartotojams. Bendrajame duomenų apsaugos reglamente numatyta, jog kiekvienu atveju turėtų būti nustatyta duomenų valdytojo

[142] ES 29 str. duomenų apsaugos darbo grupė. *Nuomonė 05/2014 dėl nuasmeninimo metodų*, 0829/14/LT WP216, p. 13.
[143] FINCK, Michele. *Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law*? Panel for the Future of Science and Technology (STOA), European Parliament Research Service (EPRS), July 2019, p. 3.

atsakomybė už bet kokį duomenų valdytojo arba jo vardu vykdomą asmens duomenų tvarkymą (Bendrojo duomenų apsaugos reglamento preambulės 74 p.). Dėl minėto „blockchain“ technologijos pobūdžio, sunku nustatyti kas tokioje situacijoje yra laikomi duomenų valdytojais ir kas turėtų prisiimti atsakomybę už tokį asmens duomenų tvarkymą. Dar daugiau, tampa sudėtinga įgyvendinti ir Bendrajame duomenų apsaugos reglamento 5 straipsnio 2 dalyje numatytą atskaitomybės principą, pagal kurį duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi visų, su asmens duomenų tvarkymu susijusių, principų, ir turi sugebėti įrodyti, kad jų yra laikomasi kai to prašoma.

Pabrėžtina, jog kai kuriais atvejais, „blockchain“ technologija yra visiškai nesuderinama su Bendruoju duomenų apsaugos reglamentu. Pavyzdžiui, Bendrojo duomenų apsaugos reglamento 17 straipsnyje numatyta duomenų subjekto teisė reikalauti ištrinti jo asmens duomenis. „Blockchain“ technologijos pagrindas yra transakcijų duomenų kaupimas bei saugojimas, įskaitant ir asmens duomenis. Šiais duomenimis yra užtikrinamas „blockchain“ technologijos stabilumas bei vientisumas. Be to, užfiksuotų transakcijų duomenys „blokų“ grandinėje turi įtakos vėlesniems skaitmeniniams įrašams, todėl, minėtos duomenų subjekto teisės įgyvendinimas gali privesti prie to, jog „blockchain“ technologija taps visiškai neefektyvi[144]. Atsižvelgus į tai, vis dar neaišku kaip šios technologijos kontekste interpretuoti reikalavimą ištrinti asmens duomenis.

Apibendrinant, naudojant „blockchain“ technologiją susiduriama su iššūkiais asmens duomenų apsaugos teisės srityje, o kai kurie šios technologijos aspektai yra visiškai nesuderinami su duomenų subjekto teisėmis, numatytomis Bendrajame duomenų apsaugos reglamente.

[144] *Ibid*., p. 4.

3.5. ES Bendrojo duomenų apsaugos reglamento taikymo iššūkiai ir ateities perspektyvos ketvirtojoje pramonės revoliucijoje

Ketvirtosios pramonės revoliucijos technologijos, tokios kaip: didieji duomenys, dirbtinis intelektas, daiktų internetas, „blockchain“ technologija, ir t.t. smarkiai plečia informacinių technologijų ribas ir yra veiksmingos priemonės našumui bei produktyvumui didinti. Naujųjų technologijų vystymasis ir pritaikymas įvairiose gyvenimo srityse ženkliai prisideda prie ekonomikos skatinimo ir tampa konkurenciniu šalių pranašumu[145]. Pradedant nuo virtualios realybės, veidų bei balso atpažinimo, savavaldžių automobilių, kuriems nereikalingas vairuotojas[146], baigiant išankstiniu sudėtingų ligų numatymu bei epidemijų prognozavimu[147]. Visa tai prisideda prie visuomenės gerovės kūrimo. Daugelis pranašauja, kad nebus nė vienos srities, kurioje nereiks duomenų apsaugos pagrindų, nes visos gyvenimo ir profesinės veiklos sritys priklausys nuo duomenų[148]. Kitaip tariant, Ketvirtosios pramonės revoliucijos pasaulis bus duomenų pasaulis[149]. Atsižvelgus į tai, pavojus žmogaus privatumui bei asmens duomenims išliks viena didžiausių grėsmių naujųjų technologijų amžiuje.

Bendrasis duomenų apsaugos reglamentas yra įrankis, kuris siekia užtikrinti duomenų subjektų teisių įgyvendinimą bei apsaugoti nuo bet kokių asmens duomenų apsaugos pažeidimų. Nepaisant to, kai kurie mokslininkai mano, jog dabartinis asmens duomenų apsaugos teisinis reguliavimas gali užkirsti kelią naujųjų technologijų pažangai bei

---

[145] LI, He; YU, Lu; HE, Wu. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 2019, VOL. 22, NO. 1, p. 1–6.

[146] Kalifornijos valstijos Motorizuotų transporto priemonių departamentas. DMV Issues Permit Authorizing Waymo to Test Driverless Vehicles in Santa Clara County (pranešimas spaudai). 2018 m. spalio 30 d. [interaktyvus] Prieiga per internetą: https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/2018/2018_81>.

[147] GARATTINI, Chiara; RAFFLE, Jade; et. Al. Big Data Analytics, Infectious Diseases and Associated Ethical Impacts. [interaktyvus]. Prieiga per internetą: https://www.ncbi.nlm.nih.gov/pubmed/?term=Raffle%20J%5BAuthor%5D&cauthor=true&cauthor_uid=31024785>.

[148]ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 318.

[149] SCHWABB, Klaus; DAVIS Nicholas. Shaping the Fourth Revolution. Portfolio Penguin. 2018, p. 19-22.

neišvengiamai padidinti šių technologijų kūrimo sąnaudas.[150] Pavyzdžiui, formalūs Bendrojo duomenų apsaugos reglamento reikalavimai, kuriais įgyvendinamos duomenų subjekto teisės bei duomenų minimizavimo principas, gali ženkliai sumažinti didžiųjų duomenų analizės kokybę ir stipriai pakenkti tokioms technologijų milžinėms kaip „Google“ ar „Facebook“, kurių verslo modelis ir paremtas asmens duomenų rinkimu bei analize, siekiant pateikti duomenų subjektams suasmenintą tikslinę reklamą[151]. Taigi, kyla iššūkių tiek tinkamam Bendrojo duomenų apsaugos reglamento įgyvendinimui, tiek tolimesniam ketvirtosios pramonės revoliucijos technologijų vystymuisi. Atsižvelgus į šiame darbe minėtus pavyzdžius bei ketvirtosios pramonės revoliucijos technologijų keliamus pavojus asmens duomenims, galima teigti, jog ateityje duomenų apsaugos teisė taps viena pagrindinių teisės sričių, o Bendrasis duomenų apsaugos reglamentas atliks ypatingai svarbų vaidmenį šioje srityje[152]. Nuo to kaip bus aiškinamas ir taikomas šis teisės aktas bei įgyvendinami jame numatyti reikalavimai, priklausys ne tik duomenų subjektų teisių bei laisvių apsauga, bet ir naujųjų technologijų pažanga bei tolimesnis jų vystymasis. Šiuo atveju, labai svarbu atrasti balansą tarp tinkamo asmens duomenų apsaugos užtikrinimo ir ketvirtosios pramonės revoliucijos technologijų teikiamos naudos bei žadamų perspektyvų. Jei asmens duomenų apsaugos teisės interpretavimas bus pernelyg griežtas, naujosios technologijos patirs stagnaciją, o tai gali neigiamai paveikti ekonomikos ir verslo plėtrą bei kitas svarbias gyvenimo sritis. Tačiau, jei asmens duomenų apsaugos teisinis reguliavimas bus pernelyg lankstus ir atlaidus duomenų valdytojams, stipriai nukentės duomenų subjekto teisės ir laisvės. Svarbu paminėti, jog ketvirtosios pramonės revoliucijos pasaulyje, duomenys yra laikomi viena didžiausių

[150] LI, He; YU, Lu; HE, Wu. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 2019, VOL. 22, NO. 1, p. 3.
[151] HOUSER, Kimberly; VOSS, Gregory. GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law & Technology* 25-1, 2018, p. 1-67 [interaktyvus]. Prieiga per internetą: https://ssrn.com/abstract=3212210.
[152] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 322.

vertybių[153]. Bendrasis duomenų apsaugos reglamentas numato, jog asmens duomenys turėtų būti tvarkomi taip, kad tai pasitarnautų žmonijai (Bendrojo duomenų apsaugos reglamento preambulės 4 p.). Atsižvelgus į tai, duomenų apsaugos teisė turi būti plėtojama, aiškinama ir taikoma taip, kad suteiktų duomenų subjektams apsaugą nuo realių pavojų, kylančių duomenų tvarkymo veikloje[154], tačiau nebūtų per daug formaliai interpretuojama.

Pabrėžtina, jog teisė į asmens duomenų apsaugą nėra absoliuti; ji turi būti vertinama atsižvelgiant į jos visuomeninę paskirtį ir derėti su kitomis pagrindinėmis teisėmis, remiantis proporcingumo principu. Atitinkamai, Europos Sąjunga, norėdama neatsilikti ir konkuruoti su kitomis valstybėmis naujųjų technologijų srityje, turi įvertinti ir tai, jog tokios valstybės, kaip Kinija ar JAV, neturi tokio griežto duomenų apsaugos teisinio reguliavimo, todėl gali kurti gerokai pažangesnes technologijas ir pralenkti Europos Sąjungą daugelyje strategiškai svarbių sričių.

Taip pat, ypatingai svarbu skatinti visuomenės sąmoningumą duomenų apsaugos teisės srityje. Visuomenė turėtų labiau domėtis savo teisėmis bei laisvėmis šioje srityje bei geriau suvokti grėsmes, kurias gali sukelti asmens duomenų apsaugos pažeidimai. Daugelis asmenų nesidomi ir neskaito įmonių pateiktų privatumo sąlygų ar kitos informacijos susijusios, su jų asmens duomenų tvarkymu. Dažnai ši informacija duomenų subjektams pateikiama sunkiai suprantama forma bei visiškai nepatraukliu būdu. Tyrimai rodo, kad vartotojai neskaito tokio pobūdžio tekstų, nes tai padaryti užtrunka pernelyg daug laiko. Nustatyta, jog perskaityti visas per metus pateiktas privatumo sąlygas bei taisykles, duomenų subjektams užtruktų maždaug 200 valandų[155]. Atsižvelgus į tai, reikalingas asmens duomenų apsaugos teisės reguliavimo ir aiškinimo supaprastinimas, pateikiant asmens duomenų apsaugos teisinio reguliavimo gaires,

[153] SCHWAB, Klaus. The Fourth Industrial Revolution. *World Econimic Forum*, 2016, p. 96.
[154]ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019, p. 327.
[155] Aleecia McDonald and Lorrie Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S 543.

kuriose būtų apibūdintos realios asmens duomenų tvarkymo situacijos bei šio teisinio reguliavimo aktualijos[156]. Atitinkamai, valstybės turėtų suteikti pakankamai finansinių bei žmogiškųjų išteklių duomenų apsaugos priežiūros institucijoms, kadangi šių institucijų, įgaliotų visiškai nepriklausomai atlikti savo užduotis ir vykdyti savo įgaliojimus, įsteigimas valstybėse narėse yra viena iš esminių fizinių asmenų apsaugos tvarkant jų asmens duomenis dalių (Bendrojo duomenų apsaugos reglamento preambulės 117 p.).

Dar daugiau, duomenų valdytojams ar tvarkytojams Bendrajame duomenų apsaugos reglamente numatytų reikalavimų įgyvendinimas reikalauja nemenko organizacinio pasiruošimo bei didelių kaštų, pasitelkiant pakankamai sudėtingus procesus, kuriuose susijungia daugelis skirtingų sričių (pvz., teisė, informacinės technologijos, žmogiškųjų išteklių valdymas ir t.t.). Šių procesų įgyvendinimas tampa komplikuotas, kadangi nėra pakankamai aišku, kaip ir kokiais būdais tai atlikti. Kitaip tariant, Bendrasis duomenų apsaugos reglamentas pateikia nemažai abstrakčių, individualaus vertinimo reikalaujančių ir dėl to daug neaiškumo keliančių nuostatų, tokių kaip: „asmens duomenų tvarkymas laikomas teisėtu, jei tvarkyti duomenis būtina siekiant teisėtų duomenų valdytojo arba trečiosios šalies interesų, išskyrus atvejus, kai tokie duomenų subjekto interesai arba pagrindinės teisės ir laisvės, dėl kurių būtina užtikrinti asmens duomenų apsaugą, yra už juos viršesni“[157]. Taigi, kyla klausimas: kada duomenų valdytojo interesas yra viršesnis už duomenų subjekto interesus? Bendrojo duomenų apsaugos reglamento 5 straipsnio 1 dalyje numatyta, kad „asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas.“[158]. Šiuo atveju, kyla klausimas: kada

[156] KUNER, Christopher. The ‘Internal Morality’ of European Data Protection Law (November 24, 2008). [interaktyvus, žiūrėta 2020 m. kovo 18 d.] Prieiga per internetą: https://ssrn.com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797.
[157] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas), 6str. 1 d. f p.
[158] *Ibid.*, 5 str. 1 d. e p.

laikoma, jog duomenų valdytojas tinkamai įgyvendino technines ar organizacines asmens duomenų apsaugos priemones? Dėl šios priežasties, nenuostabu, kad daugelis duomenų valdytojų ir tvarkytojų gali susidurti su tinkamo asmens duomenų apsaugos teisinio reguliavimo interpretavimo bei taikymo problemomis. Situacijos nelengvina ir tai, jog duomenų apsaugos priežiūros institucijos turi plačią diskrecinę laisvę spręsti dėl sankcijų už duomenų apsaugos pažeidimus ir jų dydžio skyrimo. Atsižvelgus į Bendrojo duomenų apsaugos reglamento sudėtingumą bei abstraktumą, būtinas efektyvus bendradarbiavimas tarp priežiūros institucijų ir duomenų valdytojų. Duomenų apsaugos priežiūros agentūros turėtų padėti duomenų valdytojams, paaiškinant kaip tinkamai įgyvendinti abstrakčius bei individualaus vertinimo reikalaujančius duomenų apsaugos teisės reikalavimus, o ne iškart grasinti milžiniškomis sankcijomis. Tik tokiu būdu galima tikėtis efektyvaus duomenų subjektų teisų užtikrinimo bei tinkamo šio teisės akto įgyvendinimo.

Nepaisant visų išvardintų Bendrojo duomenų apsaugos reglamento teisinio reguliavimo iššūkių, sugriežtindamas duomenų apsaugos teisinį reguliavimą bei sustiprinęs duomenų subjektų teises, Bendrasis duomenų apsaugos reglamentas iš esmės keičia požiūrį į duomenų apsaugą bei skatina duomenų apsaugos teisės globalizaciją. Atsižvelgus į tai, negalima paneigti fakto, jog ketvirtąją pramonės revoliuciją bei asmens duomenų apsaugos teisę sieja ypatingai glaudus ryšys, kadangi Bendrasis duomenų apsaugos reglamentas ir, apskritai, asmens duomenų apsaugos teisė bei ketvirtosios pramonės revoliucijos technologijos reikšmingai įtakoja viena kitos vystymąsi. Dėl šios priežasties, asmens duomenų apsaugos teisė ateityje taps viena pagrindinių teisės sričių, o Bendrasis duomenų apsaugos reglamentas atliks svarbų vaidmenį formuojant asmens duomenų apsaugos teisę ne tik Europos Sąjungoje, bet ir visame pasaulyje.

IŠVADOS

1. Asmens duomenų apsaugos teisė visuomet buvo glaudžiai susijusi su mokslo bei technologijų raida. XIX a. mokslo bei technikos išradimai, pagerinę visuomenės gyvenimo sąlygas bei paskatinę civilizacijos vystymąsi, įtakojo „teisės į privatumą“ kaip savarankiškos žmogaus teisės visuotinį pripažinimą ir įtvirtinimą tarptautiniuose teisės aktuose, o XX a. antrojoje pusėje įvykusi informacinių technologijų revoliucija, kurios dėka atrasti nauji būdai kaip rinkti, kaupti bei saugoti asmens duomenis, buvo viena iš priežasčių, lemiančių asmens duomenų apsaugos teisės koncepcijos susiformavimą bei tolimesnį vystymąsi. Vykstant nuolatinei mokslo bei technologijų pažangai, atitinkamai kinta ir asmens duomenų apsaugos teisinis reguliavimas.
2. Bendruoju duomenų apsaugos reglamentu siekiama užtikrinti laisvą bei saugų asmens duomenų judėjimą Europos Sąjungoje bei sustiprinti duomenų subjektų apsaugą nuo ketvirtosios pramonės revoliucijos technologijų keliamų pavojų. Kitaip tariant, šis teisės aktas sukurtas kaip atsakas į vis didėjantį asmens duomenų tvarkymo mastą, kurį įgalino naujausios technologijos ir kuris gali sukelti itin neigiamus padarinius duomenų subjektams.
3. Neatskiriama ketvirtosios pramonės revoliucijos dalis yra didžiųjų duomenų analizė, apimanti ir asmens duomenų tvarkymą. Atliekant didžiųjų duomenų analizę, susiduriama su iššūkiais asmens duomenų apsaugos srityje, įskaitant: asmens duomenų kontrolės stoką, asmens duomenų tvarkymo skaidrumo užtikrinimą, pakartotinio duomenų subjekto identifikavimo bei profiliavimo keliamus pavojus duomenų subjektų teisėms ir pan. Todėl, kaip niekad svarbu tinkamai interpretuoti bei taikyti Bendrąjį duomenų apsaugos reglamentą, siekiant veiksmingai apsaugoti duomenų subjektų teises bei teisėtus interesus.

4. Kadangi dirbtinio intelekto veikimas yra paremtas automatiniu sprendimų vykdymo procesu, kuris naudoja didelį kiekį asmens duomenų, netinkamas ar neteisėtas toko pobūdžio asmens duomenų tvarkymas, gali sukelti itin neigiamas pasekmes duomenų subjektams. Didžiausias iššūkis su kuriuo susiduriama taikant Bendrąjį duomenų apsaugos reglamentą dirbtinio intelekto technologijai, yra duomenų subjektų teisių, susijusių su automatiniu sprendimų vykdymu, probleminiai aspektai, dėl kurių gali būti ne tik apribojamas dirbtinio intelekto naudojimas, bet ir užkertamas kelias tolimesnei dirbtinio intelekto pažangai.
5. Viena iš greičiausiai besivystančių ir didžiausią potencialą turinčių ketvirtosios pramonės revoliucijos inovacijų yra daiktų internetas, apimantis išmaniuosius įrenginius, kurie, naudodami interneto tinklus, sąveikauja tarpusavyje, tvarko bei keičiasi asmens duomenimis. Pagrindiniai iššūkiai, su kuriais susiduriama asmens duomenų apsaugos srityje, taikant daiktų interneto technologiją, yra asmens duomenų kontrolės stoka, duomenų subjekto sutikimo kokybė bei duomenų subjektų profiliavimas.
6. Dėl specifinio „blockchain“ technologijos pobūdžio, susiduriama su asmens duomenų apsaugos teisinio reguliavimo problematika, įskaitant duomenų valdytojų nustatymą ir jų atsakomybės už asmens duomenų tvarkymą paskirstymą bei tinkamą atskaitomybės principo įgyvendinimą, o kai kurie šios technologijos aspektai, yra visiškai nesuderinami su duomenų subjektų teise ištrinti asmens duomenis, kuri numatyta Bendrajame duomenų apsaugos reglamente.
7. Nuo to kaip bus aiškinamas ir taikomas Bendrasis duomenų apsaugos reglamentas bei įgyvendinami jame numatyti reikalavimai, priklausys ne tik asmens duomenų apsaugos teisinio reguliavimo efektyvumas, bet ir ketvirtosios pramonės revoliucijos technologijų pažanga ir tolimesnis jų vystymasis. Jei asmens duomenų apsaugos teisės

interpretavimas bei taikymas bus pernelyg griežtas, naujosios technologijos patirs stagnaciją, o tai gali neigiamai paveikti ekonomikos ir verslo plėtrą bei kitas svarbias visuomenės gyvenimo sritis. Tačiau, jei Bendrojo duomenų apsaugos reglamento taikymas bus pernelyg lankstus ir atlaidus duomenų valdytojams, stipriai nukentės duomenų subjekto teisės bei jų asmens duomenų apsauga.

LITERATŪROS BEI KITŲ ŠALTINIŲ SĄRAŠAS

Norminiai teisės aktai:

Tarptautiniai teisės aktai:

1. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006, Nr. 68-2497.
2. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*. 1995, Nr.40-98.
3. Tarptautinis pilietinių ir politinių teisių paktas. *Valstybės žinios*, 2002-08-02, Nr. 77-3288.
4. 1980 m. Ekonominio bendradarbiavimo ir plėtros organizacijos (EBPO) gairės dėl privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių [interaktyvus, žiūrėta 2020 m. vasario 21 d.]. Prieiga per internetą: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.
5. 1981 m. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. *Valstybės žinios*. 2001, Nr. 32-1059.

Europos Sąjungos teisės aktai:

6. Europos Sąjungos sutarties suvestinė redakcija. OJ 2007, C 306/13-46.102.
7. Sutarties dėl Europos Sąjungos veikimo suvestinė redakcija. OJ 2007, C 306/47-200.
8. 2016 m. balandžio 27 d. Europos Sąjungos Reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo.
9. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, Specialusis leidimas, OL L 281, p. 1-31.
10. 2000 m. gruodžio 18 d. Europos Parlamento ir Tarybos reglamentas (EB) Nr. 45/2001 dėl asmenų apsaugos Bendrijos institucijoms ir įstaigoms tvarkant asmens duomenis ir

laisvo tokių duomenų judėjimo (ES institucijų duomenų apsaugos reglamentas). OL L 8, 2001 01 12, p. 1-22.

11. 2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje. OL L 201, 2002 07 31, p. 1–47.
12. Europos Sąjungos pagrindinių teisių chartija, 2012/C 326/02.

Lietuvos Respublikos teisės aktai:

13. Lietuvos Respublikos elektroninių ryšių įstatymas. *Valstybės žinios*, 2004, Nr. 69-2382.
14. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, Nr. 63-1479.
15. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo Nr. I-1374 pakeitimo įstatymas, *TAR*, 2018-07-11, Nr. 11733.

Specialioji literatūra:

16. ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija. *Registrų centras*, 2019.
17. KUNER, Christopher. European Data Protection Law. Corporate Regulation and Compliance. *Oxford University Press*, 2 edition, 2007.
18. KUNER, Christopher. The EU General Data Protection Regulation (GDPR): A Commentary. *Oxford University Press*, 2020.
19. BYGRAVE, Lee Andrew. Data Privacy Law: An International Perspective. *Oxford University Press*, 1 edition, 2014.
20. LINDSKEY, Orla. The Foundations of EU Data Protection Law. *Oxford University Press*, 2015.

21. CAREY, Peter. Data Protection - A Practical Guide to UK and EU Law. *Oxford University Press*, 5th Edition, 2018.
22. SCHWAB, Klaus. The Fourth Industrial Revolution. *Currency*, 2017.
23. ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. *Teisė*, 2017, t. 103, p. 45–54.
24. CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126-148.
25. PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174.
26. SAVUKYNAS, Raimundas; MARCINKEVIČIUS, Virginijus. Daiktų interneto objektų identifikavimo metodų palyginimas. *Informacijos mokslai*. 2017, Nr. 78, p. 67.
27. KOTSCHY, Waltraut. The proposal for a new General Data Protection Regulation – problems solved? *International Data Privacy Law,* 2014, Vol. 4, Issue 4, p. 274-281 [interaktyvus, žiūrėta 2020 m. kovo 12 d.]. Prieiga per internetą: https://academic.oup.com/idpl/article/4/4/274/2569062.
28. KUNER, Christopher; CATE H. Fred; MILLARD, Christopher; SVANTESSON Dan; JERKER, Dan. The challenge of 'big data' for data protection. *International Data Privacy Law*, Volume 2, Issue 2, May 2012, p. 47–49 [interaktyvus, žiūrėta 2020 m. kovo 12 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ips003.
29. RUBINSTEIN, Ira S. Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law,* Volume 3, Issue 2, May 2013, p. 74–87 [interaktyvus, žiūrėta 2020 m. kovo 12 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ips036.
30. KUNER, Christopher. The 'Internal Morality' of European Data Protection Law (November 24, 2008). [interaktyvus, žiūrėta 2020 m. kovo 18 d.] Prieiga per internetą: https://ssrn.com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797.

31. SVANTENSSON, Dan. The extraterritoriality of EU data privacy law - its theoretical justification and its practical effect on U.S. businesses. *Stanford Journal of International Law* 50(1), 2013, p. 53-117.
32. MAYER-SCHÖNBERGER, Viktor; PADOVA, Yann. Regime Change? Enabling Big Data through Europe's New Data Protection Regulation. *The Columbia Science and Technology law review*, 2016, p. 1-334.
33. MAYER-SCHONBERG, V; CUKIER, K. Big Data: A Revolution That Will Transform How We Live, Work and Think, *London: John Murray*, 2013, p. 73.
34. HUMERICK, Matthew. Taking AI Personally: How the E.U. Must Learn to Balance the Interests of Personal Data Privacy and Artificial Intelligence. *Santa Clara High Technology Law Journal*, Vol. 34, Issue 4, Article 3, 2018, p. 395-418 [interaktyvus, žiūrėta 2020 m. vasario 24 d.]. Prieiga per internetą: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1633&context=chtlj.
35. HOUSER, Kimberly; VOSS, Gregory. GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy? *Richmond Journal of Law & Technology* 25-1, 2018, p. 1-67 [interaktyvus, žiūrėta 2020 m. vasario 24 d.]. Prieiga per internetą: https://ssrn.com/abstract=3212210.
36. KUNER, Christopher; SVANTESSON, Dan; CATE, H. Fred; LYNSKEY, Orla; MILLARD, Christopher. Machine learning with personal data: is data protection law smart enough to meet the challenge? *International Data Privacy Law*, 2017, Vol. 7, No. 1, p. 1-2.
37. BUTTERWORTH, Michael. The ICO and artificial intelligence: The role of fairness in the GDPR framework. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2018, p. 1-2.

38. WATCHER, Sandra. The GDPR and the Internet of Things: A Three-Step Transparency Model. *Law, Innovation and Technology*, Volume 10, 2018 - Issue 2, p. 266-294.

39. LI, He; YU, Lu; HE, Wu. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management,* 2019, VOL. 22, NO. 1, p. 1–6 [interaktyvus, žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą:https://www.tandfonline.com/doi/pdf/10.1080/1097198X.2019.1569186?needAccess=true.

40. BUTTARELLI, Giovanni. The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, Volume 6, Issue 2, May 2016, p. 77–78 [interaktyvus, žiūrėta 2020 m. kovo 14 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipw006.

41. PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, 2018, VOL. 10, NO. 1, p. 40–81 [interaktyvus, žiūrėta 2020 m. vasario 23 d.]. Prieiga per internetą: https://www.tandfonline.com/doi/pdf/10.1080/17579961.2018.1452176?needAccess=true.

42. KUNER, Christopher; JERKER, Dan; SVANTESSON, Dan; CATE, H. Fred; LYNSKEY, Orla; MILLARD, Christopher; LOIDEAIN, Ni Nora. The GDPR as a chance to break down borders. *International Data Privacy Law*, Volume 7, Issue 4, November 2017, p. 231–232 [interaktyvus, žiūrėta 2020 m. vasario 23 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipx023.

43. TENE, Omer. Privacy: The new generations. *International Data Privacy Law*, Volume 1, Issue 1, February 2011, p. 15–27 [interaktyvus, žiūrėta 2020 m. vasario 23 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipq003.

44. KUNER, Christopher; CATE, Fred; LYNSKEY, Orla; , MILLARD, Christopher; LOIDEAIN, Ni Nora, SVANTESSON, Dan. Blockchain versus data protection. *International Data Privacy Law*, Volume 8, Issue 2, May 2018, p. 103–104 [interaktyvus, žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: https://doi.org/10.1093/idpl/ipy009.
45. ZARSKY, Tal. Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017 [interaktyvus, žiūrėta 2020 m. kovo 15 d.]. Prieiga per internetą: https://ssrn.com/abstract=3022646
46. ONIK, Mehedi Hassan; KIM, Chul-Soo; YANG, Jinhong. Personal Data Privacy Challenges of the Fourth Industrial Revolution. *International Conference on Advanced Communications Technology (ICACT)*, Conference Paper, February 2019, p. 635.
47. OHM, Paul. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 2010, 57 *UCLA Law Review* 1701, University of Colorado Law Legal Studies Research Paper No. 9-12.
48. WATCHER, Sandra. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Computer Law & Security Review*, 32 (2018).

Teismų praktika:

49. Europos Sąjungos Teisingumo Teismo 2014 m. gegužės 13 d. sprendimas byloje C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.
50. Europos Sąjungos Teisingumo Teismo 2016 m. spalio 19 d. sprendimas byloje C-582/14 Patrick Breyer prieš Vokietijos Federacinę Respubliką.

51. Europos Sąjungos TeisingumoTeismo 2019 m. rugsėjo 24 d. sprendimas byloje C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)
52. Europos Sąjungos Teisingumo Teismo 2017 m. kovo 9 d. sprendimas byloje C-398/15 Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni.
53. Europos Sąjungos Teisingumo Teismo 2017 m. gruodžio 20 d. sprendimas byloje C-434/16 Peter Nowak v Data Protection Commissioner.

Soft law šaltiniai:

54. Article 29 Data Protection Working Party. *Opinion 4/2007 on the concept of personal data.* Nr. 01248/07/EN WP 136, p. 1-26.
55. ES 29 str. duomenų apsaugos darbo grupė. *2013 m. balandžio 2 d. Nuomonė dėl tikslo ribojimo*. Nr. WP 203 [interaktyvus, žiūrėta kovo 16 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf .
56. ES 29 str. duomenų apsaugos darbo grupė. 2018 m. balandžio 10 d. *Gairės dėl sutikimo pagal Reglamentą 2016/679.* Nr. 17/EN WP 259 rev.01, p. 1-30.
57. European Data Protection Board. *Guidelines 3/2019 on processing of personal data through video devices.* Version for public consultation. Adopted on 10 July 2019 [interaktyvus, žiūrėta č020 m. kovo 16 d.]. Prieiga per internetą: https://edpb.europa.eu/our-work-tools/public-consultations/2019/guidelines-32019-processing-personal-data-through-video_en.
58. European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3).* Version 2.0, 12 November 2019 [interaktyvus, žiūrėta 2020 m.

vasario 15 d.]. Prieiga per internetą: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en.

59. ES 29 str. duomenų apsaugos darbo grupė. *2017 m. balandžio 4 d. Poveikio duomenų apsaugai vertinimo (PDAV) gairės, kuriomis Reglamento 2016/679 taikymo tikslais nurodoma, kaip nustatyti, ar duomenų tvarkymo operacijos gali sukelti didelį pavojų*. Nr. 17/LT WP 248, 1-oji peržiūrėta versija, p. 1-25.
60. ES 29 str. duomenų apsaugos darbo grupė. 2014 m. balandžio 9 d. *Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį.* Nr. 844/14/LT WP 217, p. 1-60.
61. International Conference of Data Protection and Privacy Commissioners (40th). *Declaration on ethics and data protection in artificial inteligence,* 23rd October 2018.
62. European Data Protection Supervisor. *Opinion. Meeting the challenges of big data. A call for transparency, user control, data protection by design and accountability* [interaktyvus, žiūrėta 2020 m. kovo 16 d.]. Prieiga per internetą: https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf.
63. European Commission. *Press release. Artificial intelligence: Commission outlines a European approach to boost investment and set ethical guidelines,* 2018 [interaktyvus, žiūrėta 2020 m. kovo 17 d.]. Prieiga per internetą: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_3362

SANTRAUKA

Pastaraisiais metais sparčiai vystantis informacinėms technologijoms bei plečiantis skaitmeninei rinkai, pradėta kalbėti apie ketvirtosios pramonės revoliucijos pradžią. Atsižvelgus į naujųjų technologijų keliamus pavojus asmens duomenų apsaugai, 2018 m. gegužės 25 d. Europos Sąjungoje įsigaliojo Bendrasis duomenų apsaugos reglamentas. Vis labiau didėjant duomenų tvarkymo mastams, kyla daugelis klausimų dėl tolimesnio asmens duomenų apsaugos užtikrinimo naujųjų technologijų amžiuje. Todėl šio darbo tikslas išnagrinėti Bendrojo duomenų apsaugos reglamento reikšmę bei įtaką naujųjų technologijų pažangai ir nustatyti jo santykį su ketvirtąja pramonės revoliucija. Šio darbo tyrimas atskleidė, jog Bendrasis duomenų apsaugos reglamentas buvo sukurtas kaip atsakas į ketvirtosios pramonės revoliucijos technologijų keliamus pavojus asmens duomenų apsaugai. Analizės metu nustatyta, kad taikant Bendrąjį duomenų apsaugos reglamentą ketvirtosios pramonės revoliucijos technologijoms, susiduriama su tokiais iššūkiais, kaip: asmens duomenų kontrolės stoka, skaidrumo principo įgyvendinimo problematika, duomenų subjekto sutikimo kokybė, pakartotinio duomenų subjekto identifikavimo bei profiliavimo keliami pavojai, duomenų subjektų teisių, susijusių su automatiniu sprendimų vykdymu, tinkamas įgyvendinimas. Atsižvelgus į tai, kaip bus aiškinamas ir taikomas Bendrasis duomenų apsaugos reglamentas, priklausys ne tik duomenų subjektų teisių apsauga, bet ir ketvirtosios pramonės revoliucijos technologijų pažanga bei tolimesnis vystymasis. Dėl šios priežasties, Bendrasis duomenų apsaugos reglamentas atliks ypatingai svarbų vaidmenį formuojant asmens duomenų apsaugos teisę ne tik Europos Sąjungoje, bet ir visame pasaulyje.

SUMMARY

With the rapid development of information technology and digital development in recent years, scientists have begun to talk about the beginning of the Fourth Industrial Revolution. Taking into account the dangers of new technologies to the protection of personal data, on 25th of May 2018, The General Data Protection Regulation has entered into force in the European Union. With the increasing scale of data processing, many questions arise regarding the further protection of personal data in the age of new technologies. Therefore, the aim of this thesis is to examine the significance and impact of the General Data Protection Regulation on the development of new technologies and to determine its relationship with the Fourth Industrial Revolution.

The analysis reveals that the General Data Protection Regulation was developed in response to the risks to personal data protection posed by the technologies of the Fourth Industrial Revolution. Therefore, the application of the General Data Protection Regulation to the technologies of the Fourth Industrial Revolution raises challenges such as: lack of control over personal data, problems with transparency, quality of data subject consent, risks of re-identification and profiling of data subject, proper realization of data subjects' rights related to automatic decision-making and etc. The interpretation and application of the General Data Protection Regulation will determine not only the protection of data subjects' rights, but also the technological progress and further development of the Fourth Industrial Revolution. For this reason, the General Data Protection Regulation will play a crucial role in shaping personal data protection law not only in the European Union but also worldwide.