Vilniaus universiteto Teisės fakulteto
Viešosios teisės katedra

Ugnės Sabalytės
V kurso, Tarptautinės ir Europos Sąjungos teisės
studijų šakos studentės

Magistro darbas

Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir socialiniai tinklai

Vadovas: lekt. dr. Julius Zaleskis
Recenzentė: lekt. dr. Gintarė Surblytė-Namavičienė

Vilnius
2019

TURINYS

ĮVADAS

Informacinės technologijos jau kuris laikas tapo neatsiejama žmonių gyvenimo dalis. Ne paslaptis, jog žmonės tampa vis labiau priklausomi nuo informacinių technologijų, o spartus jų keitimasis skatina pritaikyti naują teisinį reguliavimą kylančioms problemoms spręsti. Duomenys tapo vertingu ir konkurencingu turtu, valiuta ir netgi preke. Amens duomenys visuomet turėjo komercinę vertę įmonėms, tačiau išaugęs didesnis prieinamumas prie plataus duomenų kiekio, neaiškūs duomenų tvarkymo tikslai, tapo pagrindinėmis priežastimis, kodėl siekiama užtikrinti aukštą asmens duomenų lygį.

Socialinių tinklų populiarumas vis dar auga fenomenaliu greičiu. Tyrimas parodė, kad socialinių tinklų rinkos lyderis ,,Facebook" buvo pirmasis socialinis tinklas turėjęs milijardą registruotų paskyrų, o šiuo metu jame egzistuoja maždaug 2,4 milijardo aktyvių vartotojų per mėnesį[1]. Asmeninė informacija, kurią vartotojas nurodo registruodamasis socialiniuose tinkluose, taip pat dalindamasis ar komunikuodamas su kitais vartotojais socialiniuose tinkluose ir už jų ribų, gali suteikti galimybę sukurti gausų vartotojų interesų bei veiklos pomėgių profilį. Asmeninius duomenis, skelbiamus socialinio tinklo svetainėse, trečiosios šalys gali panaudoti įvairiais tikslais, todėl tai gali nulemti tapatybės vagystes, neskaidrius rinkimų rezultatus, finansinius nuostolius ar verslo praradimą bei sumažinti įsidarbinimo galimybes.

Suaktyvėjusi globalizacija ir spartus technologijų vystymasis paskatino priimti 2016 m. Balandžio 27 d. 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 (Bendrasis duomenų apsaugos reglamentas), kuris pradėtas taikyti nuo 2018 m. gegužės 25 d. Bendrajame duomenų apsaugos reglamente numatyti išsamūs duomenų tvarkymo reikalavimai tiek privačiame, tiek viešajame sektoriuje. Siekiant tinkamai apsaugoti Europos Sąjungos (toliau – ES) piliečių asmens duomenis, Bendrasis duomenų apsaugos reglamentas nurodo, kad trečioji šalis, kuriai planuojama perduoti asmens duomenis, turi užtikrinti pagal ES standartus pakankamą duomenų apsaugos lygį. Tai itin aktualu socialinių tinklų svetainėms, kurių buveinės yra ne ES ir kurios tvarko didelius ES piliečių asmens duomenų kiekius. Bendrasis duomenų apsaugos reglamentas įpareigoja bendroves, įskaitant ir socialinius tinklus, užtikrinti duomenų subjektų teises, pritaikant privatumo politikas prie naujo

[1] CLEMENT, J. Number of Facebook users worldwide 2008-2019. Statista, 2019. [interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: < https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>.

reguliavimo, kuriame duomenų tvarkymas privalo atitikti duomenų apsaugos teisės principus bei visus Bendrajame duomenų apsaugos reglamente nustatytus reikalavimus.

Temos aktualumas. Šio darbo aktualumą nulemia tai, kad jame nagrinėjamas naujas ES teisės aktas – Bendrasis duomenų apsaugos reglamentas ir jo taikymas socialiniams tinklams. Taip pat, socialiniai tinklai „Facebook", „Whatsapp" ir „Instagram" buvo pirmieji, kurie gavo skundus dėl netinkamo duomenų tvarkymo, tik pradėjus taikyti Bendrąjį duomenų apsaugos reglamentą. Darbe didelis dėmesys skiriamas socialinių tinklų privatumo politikų analizei, siekiant išsiaiškinti, kaip socialiniai tinklai įgyvendina naująjį Reglamentą, bei kaip užtikrina jame numatytas duomenų subjekto teises. Taip pat šio darbo akualumas pasireiškia tuo, kad analizuojamos beveik visos Bendrojo duomenų apsaugos reglamento naujovės, turinčios neabejotiną reikšmę asmens duomenų apsaugai socialiniuose tinkluose.

Darbo tikslas. Atskleisti, kaip ES Bendrasis duomenų apsaugos reglamentas taikomas socialiniams tinklams.

Darbo uždaviniai.

Tikslui pasiekti keliami šie uždaviniai:

1) atskleisti pagrindinius duomenų apsaugos teisės šaltinius, reguliuojančius socialinius tinklus;
2) atskleisti asmens duomenų sampratą bei nustatyti asmens duomenų rinkimo problematiką socialiniuose tinkluose;
3) atskleisti pagrindinių duomenų apsaugos teisės principų įgyvendinimą socialiniuose tinkluose;
4) išanalizuoti populiariausių socialinių tinklų privatumo politikas, siekiant nustatyti duomenų tvarkymo pagrindų atitiktį Bendrajam duomenų apsaugos reglamentui;
5) apibrėžti pagrindines duomenų valdytojo atsakomybes pagal Bendrąjį duomenų apsaugos reglamentą ir nustatyti duomenų valdytojo vietą socialiniuose tinkluose;

Tyrimo objektas. Šio magistro darbo objektas yra Bendrasis duomenų apsaugos reglamentas ir jo taikymas socialiniuose tinkluose.

Tyrimo metodai. Darbe taikyti šie mokslinio tyrimo metodai: lyginamasis, sisteminis, loginis-analitinis. Sisteminis metodas buvo taikomas Bendrojo duomenų apsaugos reglamento normų analizei kartu su kitomis Reglamento normomis, siekiant išsiaiškinti Bendrojo duomenų apsaugos reglamento normų sistemą bei jų pritaikymą socialiniams tinklams. Lyginamasis metodas taikytas lyginant Bendrąjį duomenų apsaugos reglamentą kartu su Direktyvos 95/46/EB nuostatomis, tai leido nustatyti reikšmingus duomenų apsaugai pasikeitimus, trūkumus bei suprasti asmens duomenų teisinės apsaugos esmę.

Taip pat lyginamuoju metodu buvo lyginamos socialinių tinklų privatumo politikos su Bendruoju duomenų apsaugos reglamentu, siekiant nustatyti privatumo politikų atitiktį numatytiems reikalavimams. Loginis analitinis metodas buvo taikomas viso darbo metu, analizuojant teisės aktus, teismų praktiką bei mokslinę literatūrą.

Darbo orginalumas. Bendrojo duomenų apsaugos reglamento tyrimai dar nepasižymi mokslinės doktrinos gausa užsienyje bei Lietuvoje. Tiesa, kai kuriuos darbe nagrinėjamus aspektus, pagal anksčiau galiojusį teisinį reguliavimą, disertacijose nagrinėjo Ilona Petraitytė, analizuodama duomenų apsaugos principus[2], taip pat Inga Malinauskaitė Van de Castel analizavo duomenų subjekto teisių įgyvendinimą virtualiuose socialiniuose tinkluose[3]. Naująjį teisinį reguliavimą, pradėjus taikyti Bendrąjį duomenų apsaugos reglamentą, analizavo Julius Zaleskis, tirdamas svarbiausius Reglamento reguliavimo pokyčius[4] bei nagrinėjo duomenų apsaugos pareigūno veiklos pagrindus[5]. Be to, paminėtina visai neseniai išleista Juliaus Zaleskio monografija, kuri yra pirmoji Lietuvoje visapusiška ir išsami mokslinė studija duomenų apsaugos teisės ir Bendrojo duomenų apsaugos reglamento temomis[6]. Taip pat asmens duomenų sampratą elektroninėje erdvėje tyrė Mindaugas Civilka kartu su Lina Šlapimaite[7] bei pagrindines duomenų subjektų teises ir jų užtrikrinimą analizavo Eglė Štareikė ir Sigita Kausteklytė-Tunkevičienė[8]. Autoritetinga užsienio mokslinė doktrina dar nepasižymi visapusiška Bendrojo duomenų apsaugos reglamento analize, aptariamos tik kelios Bendrojo duomenų apsaugos reglamento nuostatos[9]. Tuo tarpu šiame darbe yra analizuojamas Bendrojo duomenų apsaugos reglamento taikymas socialiniams tinklams; analizuojama kaip asmens duomenys yra suprantami socialiniuose tinkluose, kaip jie tvarkomi, bei kokias teises užtikrina duomenų subjektams. Darbas gali būti reikšmingas tuo, kad yra mažai

[2] PETRAITYTĖ, Ilona. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
[3] MALINAUSKAITĖ-VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017.
[4] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei, Teisė, 2017, t. 103
[5] ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104.
[6] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija, VĮ Registrų centras, 2019.
[7] CIVILKA, Mindaugas. ir ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje, *Teisė*, 2015, t. 96.
[8] ŠTAREIKĖ, Eglė. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, S. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018,
[9] DE HERT, Paul; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Volume 6, Issue 3, 2016; MANTELERO, Alessandro. *The EU Proposal for a General Data Protection Regulation and the roots of the „right to be forgotten*. Elsevier: Computer law and Security review 29, 2013.

nagrinėta, kaip socialiniai tinklai užtikrina asmens duomenų apsaugą, ypatingai naujojo reguliavimo kontekste. Darbas gali būti reikšmingas organizacijoms, siekiančioms suprasti asmens duomenų teisinę apsaugą socialiniuose tinkluose; asmenims, norintiems žinoti savo teises socialinėje erdvėje, siekiant jas tinkamai naudoti.

Svarbiausi šaltiniai. Kadangi Bendrojo duomenų apsaugos reglamento teismų aiškinimo ir taikymo praktika ganėtinai negausi, o ir pačiame Reglamente nėra konkrečiai kalbama apie duomenų apsaugą socialiniuose tinkluose, todėl vienu pagrindinių darbo šaltiniu yra ES 29 str. darbo grupės nuomonė dėl internetinių socialinių tinklų. Nors ir formaliai neprivaloma, tačiau itin reikšminga medžiaga, kuria remiasi teismai formuodami praktiką. Svarbu paminėti, jog rašant darbą pagrindiniu tyrimo šaltiniu buvo ir Bendrasis duomenų apsaugos reglamentas. Taip pat buvo remiamasi kitomis ES 29 str. darbo grupės gairėmis bei Europos Komisijos komunikatais, analizuojant skirtingus Bendrojo duomenų apsaugos reglamento aspektus. Buvo analizuojama lietuvių bei užsienio autorių mokslinė doktrina bei, nors ir negausi, Europos Žmogaus Teisių Teismo bei Europos Sąjungos Teisingumo Teismo praktika.

1. SOCIALINIAI TINKLAI IR JŲ TEISINIS REGULIAVIMAS

1.1 Socialinių tinklų samprata

Socialinių tinklų populiarumas yra laikomas fenomenaliu XXI a. informacinių technologijų reiškiniu. Tai nuolat kintančios ir ypatingai dinamiškos platformos. Asmeninio turinio dalijimosi paslauga socialinius tinklus padarė itin patrauklius ir nulėmė jų milžinišką populiarumą. Vartotojai savo bei kitų varotojų profilių peržiūras supranta kaip saviraiškos būdą, tačiau tuo pačiu šie profiliai turi didžiulę ekonominę vertę[10].

Konkuruodami tarpusavyje, socialiniai tinklai kuria vis naujų funkcijų vartotojams, siekami sudaryti kuo patogesnes sąlygas bendravimui. Šie tinklai gali būti suprantami kaip socialinė struktūra, vienijanti tam tikras interesų grupes, kurių nariai (vartotojai) tarpusavyje susiję įvariais ryšiais (draugyste, giminyste, ekonominiais santykiais, religija, išsilavinimu, pomėgiais ar socialine padėtimi), motyvuoti dalytis turima informacija, diskutuoti aktualiais klausimais, pristatyti save elektroninėje erdvėje, viešai demonstruoti socialinį aktyvumą, reklamuoti verslą, ieškoti darbo, parduoti daiktus, organizuoti renginius ir kitas įvairias veiklas.

Vartotojai jungiasi prie socialinių tinklų per svarbiausią tinklo elementą - asmeninę vartotojo paskyrą. Socialinių tinklų paslauga yra nemokama, tačiau kuo daugiau asmeninės informacijos paskyroje pateikiama, tuo ji naudingesnė socialinio tinklo administracijai, kuri, pasitelkdama turima informacija, gali klasifikuoti vartotojus į tam tikrus segmentus ir siūlyti atitinkamą reklamą. Neteisėtai renkant ir netinkamai naudojant asmens duomenis gali kilti didelė grėsmė asmenų privatumui. Socialiniai tinklai asmens duomenis renka per vartotojo paskyrą, šiais duomenimis dalijasi su kitais elektroninės platformos dalyviais - bendradarbiavimo, paslaugų teikimo ar kitais pagrindais. Surinkti asmens duomenys yra naudojami analizuojant vartotojo įpročius ir elgesį platformoje, galiausiai pasiūlant individualizuotą reklamą arba socialinio tinklo bei trečiųjų šalių, kitų platformos dalyvių paslaugas vartotojui[11]. Apsilankius interneto svetainėje, siunčiami kompiuterio naudotojo duomenys (pvz., IP adresas, nustatyta kalba, laiko zona, programinė įranga, slapukai ir kt.) kelioms skirtingose valstybėse veikiančioms

[10] FELT, Adrienne. ir EVANS, David.Privacy protection for social networking APIs. Web 2.0 Security and Privacy , 2008: 1-9;
[11] MALINAUSKAITĖ-VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017, p 50.

rinkodaros, reklamos ir kita veikla besiverčiančioms bendrovėms [12]. Tokiu būdu informacija apie vartotoją tampa elektroninio verslo dalimi. Kai kurių tyrimų duomenimis, ES piliečių duomenų piniginė vertė valstybei, verslui ir piliečiams 2020 m. gali siekti 1 trilijoną eurų[13].

Prisijungęs prie socialinio tinklo, asmuo turi užpildyti anketą, kurioje pateikiama kuo daugiau asmeninės informacijos. Asmeninės anketos yra sukuriamos, kai pateikiama informacija apie asmens amžių, gyvenamąją vietą, interesus [14]. Dauguma svetainių reikalauja naudotojus įsikelti profilio nuotrauką. Yra socialinių tinklų, kurie nustato griežtus naujo vartotojo tapatybės nustatymo reikalavimus – pvz., ,,Airbnb", siekdamas patikrinti vartotojų tapatybę, pasilieka teisę paprašyti pateikti nuotrauką, esančią tapatybę patvirtinančiame dokumente, ar pateikti tapatybės kortelės nuotrauką. Be to reikalaujama atsakyti į kelis asmeninio pobūdžio klausimus, susieti savo vartotojo profilį su kito socialinio tinklo profiliu (šiuo atveju ,,Facebook Login"), pateikti telefono numerį, elektroninio pašto adresą, suteikti prieigą prie kitos paslaugos paskyros, kad būtų patikrinta asmens veikla ir duomenys joje [15]. Socialinio tinklo ,,Facebook" bendrose naudojimo sąlygose reikalaujama, kad vartotojai užsiregistruodami pateiktų savo tikrą vardą ir pavardę, lytį, elektroninio pašto adresą, sukurtų ne daugiau nei vieną asmeninę anketą, antraip ,,Facebook" pasilieka teisę panaikinti tokią anketą[16].

Siekiant išvengti privatumo pažeidimų, socialiniai tinklai suteikia galimybę vartotojams patiems nusistatyti savo privatumo nustatymus, nurodant kas gali peržiūrėti asmeninę informaciją. Tokie nustatymai leidžia vartotojams socialiniame tinkle reguliuoti savo profilio ar kitos su vartotoju susijusios informacijos matomumą ir prieinamumą. Privatumo nustatymai leidžia nustatyti, kam bus prieinama vartotojo informacija skirtingose profilio vietose (pvz., tam tikros nuotraukos, vaizdo įrašai, diskusijos ir pan.). Pavyzdžiui, ,,Facebook" privatumo nustatymuose galima kontroliuoti informaciją kiekvieno atskiro asmens atžvilgiu. Visgi socialinių tinklų privatumo nustatymai yra itin kritikuojami dėl jų valdymo mechanizmo sudėtingumo. Siekiant suvokti, kaip naudotis privatumo nustatymais, dažniausiai reikalingas susipažinimas su itin didelės apimties ar

[12] CIVILKA, Mindaugas. ir ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje, *Teisė*, 2015, t. 96, p. 126-148.
[13] BOSTON CONSULTING GROUP. *The Value of Our Digital Identy. Liberty Global*, Inc., 2012, p. 103 [interaktyvus. Žiūrėta 2019 m. kovo 10 d.]. Prieiga per internetą: <https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf>.
[14] BOYD, Danah. ir ELLISON N. B. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13, 2007, p. 210-230.
[15] Airbnb. *Terms of Service* [interaktyvus. Žiūrėta 2018-02-28]. Prieiga per internetą: <https://www.airbnb.com/terms/>.
[16] Facebook. *Terms of service. Section 3* [interaktyvus. Žiūrėta 2019-02-28]. Prieiga per internetą: <http://www.facebook.com/legal/terms>.

sudėtingu stiliumi parašytais tekstais. Nuo 2018 m. „Facebook" atliekant privatumo nustatymų pakeitimus, vadovaujantis Bendrojo duomenų apsaugos reglamento reikalavimais, buvo siekiama socialinių tinklų vartotojams paaiškinti kaip ir kokiais tikslais bei būdais jų asmens duomenys yra renkami, taip pat palengvinti vartotojų galimybę naudotis privatumo nustatymais, tačiau tai vis tiek kelia daug neaiškumų vartotojui. Privatumo nustatymo procedūra yra sudėtinga, kadangi nustatymai yra pateikiami ne vienoje vietoje, į juos patenkama spaudžiant skirtingas nuorodas, nukreipiant į naujus puslapius, bet to, dažnai nėra aišku kokį konkretų nustatymo elementą galima pakeisti[17]. Profesoriaus D. Štitilio nuomone vartotojams tinkamai suprasti bei reguliuoti privatumo nustatymus socialiniuose tinkluose trukdo tai, kad tiek kai kurių nustatymų valdymo aplinka, tiek socialinio tinklo privatumo politika yra tik anglų kalba. Vadinasi, prastai angliškai mokantiems vartotojams nėra galimybės gimtąja kalba susipažinti su privatumo politika ir privatumo nustatymais[18].

Taip pat, problema yra sutikimas ir sutikimo nebuvimas tvarkant asmens duomenis socialiniuose tinkluose, kuris privalo būti aiškus.[19] Socialiniame tinkle „Facebook" yra galimybė koreaguoti nustatymus, susijusius su profilio viešumu, informacijos bendrinimu su trečiųjų šalių programomis bei kitus parametrus. Tačiau kalbant apie duomenų politiką vartotojų pasirinkimas yra suvaržytas. Norint susikurti anketą socialiniame tinkle, privalu sutikti su jų siūloma privatumo politika. Vartotojai dalindamiesi savo asmeniniais duomenimis sunkiai gali suprasti, kuriuos ir kiek duomenų renka kuri įmonė, kam bus perduoti jų duomenys ir kokios yra sutikimo tvarkyti duomenis, pasekmės[20].

Europos Komisijos atliktame tyrime nurodyta, jog socialinių tinklų programinė įranga skiriasi pagal savo funkcionalumus ir programėles (angl. – *applications*)[21]. Akademinėje literatūroje bei tinklapiuose, kuriuose fiksuojamos didžiausios programavimo sąsajų saugyklos, yra išsskiriama pagrindinė taikomoji programavimo sąsaja API (angl. – *application programming interface*), kurios pagalba funkcionuoja daugelis virtualių

[17] KUCZERAWY, Aleksandra. ir FANNY, Coudert. Privacy Settings in Social Networking Sites: Is It Fair?*. Interdisciplinary Centre for Law & ICT (ICRI) – K.U.Leuven - IBBT, Sint-Miechielsstraat 6, 3000 Leuven, Belgum.

[18] ŠTITILIS, D. et al. Interneto ir technologijų teisė: vadovėlis. Mykolo Romerio universitetas. – Vilnius: Registrų centras, 2016. p. 374.

[19] MALINAUSKAITĖ-VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017, p. 98.

[20] Legislative intent on the 9th amendment to the German Competition Act (GWB), Bundestag printed paper 18/10207, p. 50.

[21] MARTIN, Aaron. ir VAN BAVEL, Rene. Assesing the Benefits of Social Networks for Organizations (European Commision Joint research Center, 2013).

socialinių tinklų visame pasaulyje[22]. Vienas labiausiai paplitęs būdas rinkti turinio informaciją iš virtualių socialinių tinklų yra naudojamas API[23]. Pavyzdžiui, socialiniame tinkle *Facebook* įvairios paslaugų programėlės per vartotojo paskyrą, naudojantis API technologija, gali užklausti vartotojo ir jo tinkle esančių kitų narių asmeninių duomenų. Programos kūrėjams prieinama informacija apima gyvenamuosius miestus, bendravimo nustatymus, muzikos skonį, lankytinas vietas, politines pažiūras, peržiūrimus video, funkcijos „Patinka" paspaudimus bei kitus[24]. Taigi informacija apie daugumą vartotojų yra pakankama, kad jų savininkai būtų identifikuoti, net jei jų vardas bei pavardė būtų pašalinti[25]. Tokiu būdu tiek pats socialinis tinklas, tiek trečiosios šalys ir kiti subjektai elektroninėje platformoje, pasinaudodami API technologija, surenka milžiniškus kiekius vartotojų duomenų. Išnaudodami duomenų subjektų pateiktą asmeninę informaciją, socialiniai tinklai generuoja savo pajamas, sudarydami sąlygas vystytis elektroninei reklamai ir įvairiausioms tiek savo pačių sukurtomis, tiek ir trečiųjų šalių paslaugoms[26]. Todėl panašu, kad API technologijos įdiegimas į socialinius tinklus sukūrė būdą, kaip apeiti privatumo nustatymus ir padidino riziką duomenų apsaugai.

Vienas iš teisingumo bei sąžiningumo principų koncepcijos elementų yra socialinių tinklų paslaugų teikėjų įsipareigojimas atsižvelgti į duomenų subjektų (vartotojų) interesus bei lūkesčius jų asmens duomenų tvarkymo srityje. Todėl duomenų tvarkymas socialiniuose tinkluose turėtų būti atliekamas taip, kad pavyktų išvegti nepagrįsto kišimosi į duomenų subjektų privatumą, nepagrįsto ribojimo teisės patiems nustatyti asmeninės informacijos naudojimą bei nepagrįsto perteklinės informacijos apie asmenį rinkimo.

[22] FELT, Adrienne., EVANS, David. Privacy protection for social networking APIs. Web 2.0 Security and Privacy (2008): 1-9;
BUCCAFURRI, Francesco et al. A model to support design and development of multiple-social-network applications. Elsevier: Information Sciences 331 (2016): 107.
[23] ABDESSLEM, Fehmi Ben et al. Reliable online social network data collection. Springer: Computational Social Networks: Mining and Visualization (2012): 183-202.
[24] FELT, Adrienne., EVANS, David. Privacy protection for social networking APIs. Web 2.0 Security and Privacy (2008): 1-9;
[25] SWEENEY, Latanya. Uniqueness of Simple Demographics in the U.S. Population. Technical report, Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA, 2000.
[26] MALINAUSKAITĖ-VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017, p 52.

1.2. Duomenų apsaugos teisės šaltiniai, reguliuojantys socialinius tinklus

Duomenų apsaugos teisės šaltiniai yra tai, kas įtvirtina arba atskleidžia duomenų apsaugos teisės normas[27]. Siekiant nustatyti ir išanalizuoti teisės šaltinius, reguliuojančius socialinius tinklus, pirmiausia būtina aptarti duomenų apsaugos teisės šaltinius. Asmens duomenis saugantis teisinis reguliavimas kilo iš žmogaus teisių apsaugos tarptautinėje teisėje. Asmens duomenų apsaugos teisės pradžia galima laikyti 1948 m. Visuotinę žmogaus teisių deklaraciją, kuri kvietė valsybes laikytis pagrindinių žmogaus teisių ir laisvių, o viena tokių - teisė į privatų gyvenimą (12 str.)[28]. 1950 m. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos 8 straipsnyje asmens teisė į privatumą įtvirtinta kaip pagrindinė žmogaus teisė[29]. Informacija, susijusi su asmens privačiu gyvenimu, ekonomikos kontekste tampa preke, turinčia didelę komercinę vertę[30]. Iš tikrųjų asmens duomenys tapo tokie vertingi, kad jie pradėti vadinti skaitmeninės eros nafta. Suvokiant tokios informacijos vertę, pastebint kylančias bei didėjančias grėsmes bei pasekmės duomenų saugumui buvo pradėta ieškoti būdų, kuriais būtų galima užtikrinti teisingą asmens duomenų apsaugą.

Nuo 1960 –ųjų iki 1990-ųjų pastebimas Europos valstybių narių siekis priimti bei įgyvendinti teisės aktus susijusius su asmeninės informacijos apsauga[31]. 1970 m. buvo priimtas Vokietijos Heseno žemės asmens duomenų apsaugos įstatymas, kuriuo pirmą kartą pasaulyje bandyta sureguliuoti asmens duomenų apsaugą, vėliau tuo pačiu keliu pasekė kitos šalys, tokios kaip Švedija, Jungtinės Amerikos Valstijos (toliau – JAV) bei kitos Europos valstybės, kuriose duomenų apsauga buvo įtvirtinta kaip viena pagrindinių konstitucinių teisių[32].

Vienas reikšmingiausių siekių įtvirtinti duomenų apsaugą buvo Tarptautinės ekonominio bendradarbiavimo ir plėtros organizacijos (toliau – EBPO) 1980 m. priimta Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių (toliau – EBPO gairės), kurios susistemino ir įtvirtino esminius asmens duomenų tvarkymo principus. EBPO gairės yra bene autoritetingiausias

---

[27] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius, 2019, p. 59.
[28] 1948 m. Visuotinė žmogaus teisių deklaracija. Jungtinės Tautos (JT).*Valstybės žinios*, 2006-06-17, Nr. 68-2497.
[29] 1950 m. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995-05-16, Nr. 40-987.
[30] KELLEHER, Denis., MURRAY, Karen. *IT Law in the EU*. Sweet and Maxwell, 1999, p. 221.
[31] MOORE, Nick. *Rights and Responsibilities in an Information Society*// The Journal of Information Law and Technology. No1.1998. [interaktyvus. Žiūrėta 2019 m. kovo 5 d.]. Prieiga per internetą: http://elj.warwick.ac.uk/jilt/infosoc/1998_1moor/.
[32]CATE, H. Fred. *Privacy in the information age*. 1997. [interaktyvus. Žiūrėta 2019 m. kovo 5 d.]. Prieiga per internetą: http://brookings.nap.edu/books/0815713169/32.gif.

tarptautinis duomenų apsaugos *soft law* šaltinis[33]. EBPO iš viso priėmė ir paskelbė daugiau nei 20 rekomendacijų, gairių ir kitų *soft law* šaltinių informacijos saugumo ir privatumo apsaugos klausimais. EBPO šaltiniai atskleidžia rekomenduojamus elgesio standartus informacinių sistemų ir tinklo saugumo, kriptografijos politikos, autentifikavimo vykdant elektroninę komerciją, privatumo apsaugos globaliuose tinkluose, vaikų apsaugos internete, skaitmeninių saugumo rizikų valdymo klausimais[34].

EBPO Gairės taikomos bet kokiai informacijai susijusiai su asmeniu (duomenų subjektu), kurio tapatybė yra nustatyta ar gali būti nustatyta. Taip pat taikomos tiek privačiam, tiek viešam sektoriui, visoms kompiuterizuoto asmens duomenų tvarkymo sistemoms ir priemonėms ir apima bet kokį asmens duomenų tvarkymą ar naudojimą. Gairėse įtvirtinti tokie pagrindiniai asmens duomenų tvarkymo principai:

- Asmens duomenų rinkimo apribojimo principas, reiškiantis, jog turėtų būti nustatyti asmens duomenų rinkimo apribojimai ir visi tokie duomenys turėtų būti gaunami tik teisėtomis bei teisingomis priemonėmis, o tam tikrais atvejais žinant duomenų subjektui ir gavus jo pritarimą;
- Asmens duomenų kokybės principas, reiškiantis, kad asmens duomenys turi būti tikslūs, išsamūs, nuolat atnaujinami bei susiję su tikslu, kuriam jie naudojami;
- Tikslo nustatymo principas, reiškiantis, jog tikslai, kuriais renkami asmens duomenys turi būti nurodyti ne vėliau kaip duomenų rinkimo metu, o vėlesnis jų naudojimas turi būti apribojamas šių tikslų pasiekimui ir įgyvendinimui, ar kitiems tikslams, kurie nors ir nėra nurodyti, bet yra suderinami su tais nurodytais tikslais.
- Asmens duomenų panaudojimo ribojimo principas, reiškiantis, kad asmens duomenys neturėtų būti atskleidžiami, prieinami ar kitaip naudojami bei nustatyti tikslo nustatymo principu, išskyrus atvejus, kai: a) yra duomenų subjekto sutikimas, arba b) įstatymo nustatytais atvejais;
- Saugumo užtikrinimo principas, reiškiantis, jog asmens duomenys turėtų būti apsaugoti protingomis saugumo priemonėmis nuo tokių pavojų kaip duomenų praradimas, neteisėtas priėjimas, sunaikinimas, naudojimas, keitimas ar atksleidimas;

[33]Ekonominio bendradarbiavimo ir plėtros organizacijos informacijos saugumo ir privatumo darbo grupė. Inventory of instruments and mechanisms, contributing to the implementation and enforcement of the OECD Privacy Guidelines on Global Networks, Paris, 1999, p. 10 [interaktyvus. Žiūrėta 2019 m. Balandžio 3 d.] prieiga per internetą: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(98)12/FINAL&docLanguage=En.

[34] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius, 2019, p. 66.

- Atvirumo principas, reiškiantis, jog turėtų būti bendra atvirumo politika apie asmens duomenų vystymąsi, praktiką ir politiką. Turėtų būti prieinamos priemonės, leidžiančios nustatyti asmens duomenų buvimą ir pobūdį bei pagrindinius jų naudojimo tikslus, taip pat duomenų valdytojo tapatybę ir jo buvimo vietą;
- Individualaus dalyvavimo principas, reiškiantis, jog asmuo turi teisę gauti iš duomenų valdytojo patvirtinimą, ar jis turi su asmeniu susijusių duomenų, taip pat asmuo turi teisę per protingą laiko tarpą gauti informaciją apie duomenis, esančius pas duomenų valdytoją, tokia forma bei būdu, kuri jam būtų suprantama;
- Atskaitomybės principas, reiškiantis, jog duomenų valdytojas privalo būti atskaitingas už tai, kaip jis laikosi priemonių, kurios įgyvendina anksčiau nurodytus principus[35].

Pagrindinė daugiašalė tarptautinė sutartis, kuria reguliuojami duomenų apsaugos klausimai - Europos Tarybos 1981 m. Strasbūro konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu Nr. 108 (toliau – ET duomenų apsaugos konvencija)[36]. Šio akto įsigaliojimas buvo vienas svarbiausių žingsnių asmens duomenų apsaugos teisės raidai. Šį privalomo pobūdžio aktą, kurį ratifikavo beveik 50 valstybių, sudarė įvairių, taip pat ir ne ES duomenų apsaugos, sistemų pagrindas[37]. Pagrindinė nuostata, kuria vadovautasi, tai siekis apsaugoti kiekvieno žmogaus pagrindines teises ir laisves, ypač teisę į privatų gyvenimą, bei teisėtą asmens duomenų tvarkymą, kuris visada turėtų atitikti tam tikras sąlygas. Konvencijoje Nr. 108 pripažįstama, kad nevaržomas ir neribojamas asmens duomenų ir informacijos perdavimas, judėjimas, neribojamas asmens teisės į informaciją realizavimas, gali neigiamai paveikti kitų fundamentalių žmogaus teisių ir laisvių apsaugą (pavyzdžiui, teisę į asmens privataus gyvenimo gerbimą, nediskriminaciją, teisingą teismo procesą ir kt.)[38]. Todėl 5 straipsnyje nustatyti pagrindiniai duomenų apsaugos principai, įskaitant reikalavimą, kad automatizuotai

[35] Ekonominio bendradarbiavimo ir plėtros organizacijos informacijos saugumo ir privatumo darbo grupė. 1980 m. Rekomendacija dėl asmens privatumo apsaugos ir asmens duomenų judėjimo tarp valstybių narių gairių [interaktyvus. Žiūrėta 2019 m. kovo 21 d.]. Prieiga per internetą: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[36] 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. Valstybės žinios, 2001-04-13, Nr. 32-1059.

[37] DE HERT, Paul; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Volume 6, Issue 3, 2016 p. 230–243. [interaktyvus. Žiūrėta 2019 m. kovo 21 d.]. Prieiga per internetą: https://academic.oup.com/idpl/article/6/3/230/2447252.

[38] 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) .Valstybės žinios, 2001-04-13, Nr. 32-1059.

tvarkomi asmens duomenys turi būti gauti ir tvarkomi sąžiningai ir teisėtai[39]. ET duomenų apsaugos konvencijoje jau buvo kalbama apie automatizuotą asmens duomenų tvarkymą bei papildomai įtraukiamas principas, reikalaujantis atitinkamų apsaugos priemonių jautriems duomenims, t. y. tokiems duomenims, kurie atskleidžia rasinę kilmę, politinius įsitikinimus, religines nuostatas ar sveikatos būklę. Tačiau, visi kiti ET duomenų apsaugos konvencijoje nurodomi principai savo esme buvo labai panašūs į numatytus EBPO privatumo gairėse. Be to, kaip buvo įtvirtinta EBPO privatumo gairėse, taip ir ET duomenų apsaugos konvencijoje, nagrinėjami tarpvalstybiniai informacijos perdavimai, todėl tai paskatino reikalauti, jog ET duomenų apsaugos konvenciją gali ratifikuoti šalys, turinčios lygiaverčius, ET duomenų apsaugos konvencijoje numatytus, duomenų apsaugos įstatymus[40].

ES lygiu duomenų apsaugos rėžimas buvo įtvirtintas priimant direktyvą 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Ji reikalavo, kad visos valstybės narės priimtų nacionalinius įstatymus, atitinkančius minimalius asmens duomenų apsaugos standartus. Direktyva 95/46/EB buvo skirta įgyvendinti du tikslus – iš vienos pusės apsaugoti fizinių asmenų pagrindines teises ir laisves, o ypač jų privatumo teisę tvarkant asmens duomenis, o iš kitos pusės – nevaržyti ir nedrausti laisvo asmens duomenų judėjimo tarp valstybių narių dėl priežasčių, susijusių su asmens duomenų apsauga[41]. Asmens duomenų apsaugos procesas ES buvo pratęstas priimant Direktyvą 97/66/EB dėl asmenų privatumo apsaugos telekomunikacijų sektoriuje, kurią nuo 2003 m. spalio 31 d. pakeitė Direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)[42].

Beje, išsamus ES duomenų apsaugos reguliavimas turėjo įtakos ir JAV reguliavimo tradicijai. Direktyvoje 95/46/EB numatyta, kad asmens duomenys trečiajai šaliai gali būti perduodami iš esmės tik tuo atveju, jei trečioji šalis užtikrina tinkamą duomenų apsaugos lygį[43]. JAV buvo traktuojama kaip neturinti atitinkamo duomenų

[39] CIVILKA, Mindaugas., et al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004, p. 107.
[40] DE HERT, Paul;PAPAKONSTANTINOU, Vagelis; The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. *Computer Law& Security Review 30* (2014) 633-642.
[41] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. *OL 2004 m. specialusis leidimas,* 13 skyrius, 15 tomas, p. 355–374.
[42] 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, p. 0037-0047.
[43] 1955 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių asmenų judėjimo. Oficialusis leidinys OJ L 281, 23/11/1995, p. 31-50.

apsaugos lygmens pagal Direktyvos 95/46/EB nuostatas, todėl buvo iškilęs klausimas dėl asmens duomenų laisvo judėjimo principo apribojimo. 1998 m. JAV Komercijos departamento pasiūlyti „Saugaus uosto" (angl. – „Safe harbor") principai, prie kurių prisijungusios JAV įmonės buvo laikomos turinčiomis tinkamą privatumo apsaugos principų laikymosi lygį[44]. ES Teisingumo Teismas *Schrems prieš Data Protection Commissioner* sprendime nurodė, jog „Saugaus uosto" sistema taikoma tik ją vykdančioms JAV įmonėms, o JAV valdžios institucijoms sistema netaikoma. Taigi šie principai buvo taikomi tik JAV įmonėms, gaunančioms asmens duomenis iš ES ir nereikalaujama, kad JAV valdžios institucijos būtų įpareigotos laikytis šių principų. Be to, ES Teisingumo Teismas nusprendė, jog „Saugaus uosto" principai nebegalioja, kadangi reikalingas išsamus tyrimas, nustatantis ar JAV užtikrina tinkamą asmens duomenų apsaugos lygį. Ši byla buvo sprendžiama po to, kai buvo atskleista, kad asmens duomenys pagal „Saugaus uosto" sistemą per socialinį tinklą „Facebook", buvo prieinami JAV nacionalinio saugumo agentūrai. Teismas motyvavo, jog reglamentavimas, leidžiantis valstybės institucijoms apskritai susipažinti su elektroninės komunikacijos turiniu, turi būti laikomas keliančiu pavojų Chartijos 7 straipsnyje garantuotos pagrindinės teisės į privatų gyvenimą esmei[45].

Reaguodama į šį sprendimą, Europos Komisija 2015 m. lapkričio 6 d. išleido komunikatą COM(2015)566 galutinis dėl asmens duomenų perdavimo iš ES į JAV pagal 95/46/EB Direktyvą ir ES Teisingumo Teismo sprendimą byloje *Schrems prieš Data Protection Commissioner*. Šiame komunikate nurodoma, kad duomenų perdavimui į trečiąsias valstybes, tokias kaip JAV, įmonės gali naudoti alternatyvius įrankius ir dėl to perdavimas gali tapti teisėtu. Tačiau kaip pagrindinis prioritetas vis dėlto išlieka poreikis susitarti su JAV dėl asmens duomenų perdavimo modelio ir sąlygų. Toks modelis turėtų užtikrinti didesnę ES piliečių duomenų apsaugą, juos perduodant į JAV. Tuo laikotarpiu, kol bus ieškoma tinkamo sprendimo, ES valstybės narės, besivadovaudamos įmonei privalomomis taisyklėmis ir standartinėmis sutarties sąlygomis, gali išduoti leidimus teikti asmens duomenis JAV[46].

[interaktyvus. Žiūrėta 2019 m. lapkričio 10 d.] Prieiga per internetą: <https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A31995L0046>.

[44] MALINAUSKAITĖ, I. *Privatumas socialiniuose tinkluose kaip įstatymo saugoma vertybė*. Social Transformations in Contemporary Society, 2015, p. 115-127.

[45] Europos Sąjungos Teisingumo Teismas. 2015 m. spalio 6 d. sprendimas *Maximillian Schrems prieš Data Protection Commissioner* Byloje C-362/14, EU:C:2015:650.

[46] Europos Komisija. Dėl asmens duomenų perdavimo iš ES į Jungtines Amerikos Valstijas pagal Direktyvą 95/46/EB, Teisingumo Teismui priėmus sprendimą byloje C-362/14 (Schrems). *Komisijos komunikatas Europos Parlamentui ir Tarybai COM(2015) 566 galutinis*, 2015, Briuselis, p. 4.

Iš visų ES duomenų apsaugos *soft law* šaltinių reikšmingiausi yra Europos duomenų apsaugos valdybos (pakeitusios anksčiau veikusią 29 str. darbo grupę) gairės, rekomendacijos ir geriausios praktikos pavyzdžiai. ES 29 str. darbo grupė išaiškino svarbiausius ES duomenų apsaugos teisės klausimus, pavyzdžiui, duomenų sampratos, duomenų valdytojų ir tvarkytojų sampratos, taikytinos teisės, sutikimo dėl duomenų tvarkymo sampratos, duomenų valdytojo teisėtų interesų sampratos, tikslo ribojimos principo, atskaitomybės principo ir kitus. Be to, ES 29 str. darbo grupė paskelbė ir autoritetingų rekomendacijų dėl specifinių BDAR nuostatų aiškinimo: duomenų apsaugos pareigūno, poveikio duomenų apsaugai vertinimo, pranešimų apie duomenų saugumo pažeidimus, automatizuoto sprendimų priėmimo ir profiliavimo, pagrindinės priežiūros institucijas ir kitas[47].

Kalbant apie socialinius tinklus, jų paprastumas naudotis, tačiau tuo pačiu ir mažas naudotojų sąmoningumas bei suvokimas apie kylančius pavojus, atskleidžiant asmeninę informaciją socialinėje erdvėje, paskatino tarptautines organizacijas bei Europos agentūras imtis veiksmų. ES tinklų ir informacijos apsaugos agentūra (toliau – ENISA) 2007 metais paskelbė dokumentą, kuriame pateikiama informacija susijusi su socialinių tinklų saugumu bei nurodomos rekomendacijos dėl jų naudojimo. Ketvirtoji pramonės revoliucija pabrėžia poreikį sustiprinti kibernetinį saugumą. Todėl ENISA aptarė pagrindines kylančias grėsmes socialinių tinklų vartotojams, viena jų, skaitmeninis duomenų rinkimas, kai socialiniuose tinkluose esančių anketų duomenys gali būti perduoti trečiosioms šalims, sukuriant skaitmeninę asmens duomenų bazę. Rekomendacijoje taip pat aptariami pavojai susiję su sunkumais ištrinti vartotojo paskyrą, veido atpažinimo funkcijos grėsme, pačių vartotojų pateikiamos informacijos gausa, galimybe nustatyti vartotojo lokaciją[48]. Akivaizdu, jog visi galioję pavojai vis dar yra aktualūs ir šių dienų asmens duomenims socialiniuose tinkluose.

2008 m. Berlyno Tarptautinė telekomunikacijų duomenų apsaugos darbo grupė (ICDPPC) priėmė memorandumą, kuriame analizuojami socialinių tinklų keliami pavojai saugumui ir pateiktos gairės paslaugų teikėjams, gavėjams (toliau – Romos memorandumas)[49]. Romos memorandume buvo pasiūlytos rekomendacijos, kuriose siūloma: daugiau skaidrumo ir informacijos vartotojams. Informacija turėtų būti pritaikyta konkretiems tikslinės auditorijos poreikiams (ypač nepilnamečiams asmenims),

[47] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius, 2019, p. 75.
[48] ENISA Position Paper No. 1. Security Issues and Recommendations for Online Social Networks. October, 2007.
[49] Berlyno tarptautinė telekomunikacijų duomenų apsaugos darbo grupė. Socialinio tinklo paslaugų privatumo atsakaita ir gairės. Romos Memorandumas. 2008 m. kovo 4 d., 675.36.5. Roma (Italy).

kad jie galėtų priimti teisingus sprendimus. Taip pat užtikrinti privatumo politiką, suteikti galimybę susikurti vartotojų anketas prisidengiant slapyvardžiu. Siūloma siekti išlaikyti vartotojų pasitikėjimą aiškia ir nedviprasmiška informacija, apie paslaugų teikėjo informacijos tvarkymą, ypatingai kai tai susiję su asmens duomenų dalijimusi su trečiosiomis šalimis. Taip pat įdiegti privatumo reikalavimus atitinkančius numatytuosius nustatymus, kad būtų pagerinta trečiųjų šalių kontrolė naudojant profilio duomenis[50].

Neabejotinai itin svarbus ir reikšmingas Direktyvos 29 straipsnio pagrindu įkurtos duomenų apsaugos darbo grupės dokumentas – Nuomonė Nr. 5/2009 dėl socialinių tinklų internete[51]. Joje išreiškiamas nemažas susirūpinimas dėl internetiniuose socialiniuose tinkluose naudojamų privatumo nustatymų. Tik nedidele vartotojų dalis, registruodamiesi socialiniuose tinkluose, atlieka kokius nors numatytųjų nuostatų keitimus. Todėl darbo grupės nuomone, internetinių socialinių tinklų teikėjai privatumo atžvilgiu turėtų teikti patogias numatytąsias nuostatas, suteikiančias galimybę vartotojams laisvai ir aiškiai leisti prieigą prie jų profilio turinio, nepasiekiamo jų pasirinktiems adresatams, ir taip sumažinti neteisėto trečiųjų šalių atiliekamo duomenų tvarkymo pavojų[52]. Darbo grupė pasiūlymų kaip to pasiekti nepateikė. Tačiau panašu, jog prisiregistruojant prie socialinio tinklo, galimybė iš karto tvarkyti privatumo nustatymus, apribojant socialinių tinklų bei trečiųjų šalių prieigą prie asmens duomenų, suteiktų daugiau aiškumo. Be to, nuomonėje teigiama, kad socialinių paslaugų teikėjai vartotojams turėtų teikti informaciją ir tinkamą įspėjimą apie privatumo riziką, kai jie įkelia duomenis į socialinių tinklų svetainę. Socialinių tinklų paslaugų teikėjai turėtų informuoti vartotojus, kad duomenų apie kitus asmenis skelbimas turėtų būti įkeltas tik su to asmens sutikimu. Socialinių tinklų svetainėje turi būti nustatyti maksimalūs laikotarpiai neaktyvių naudotojų duomenų saugojimui. Be to, socialinių tinklų operatoriai turėtų imtis atitinkamų veiksmų, kad apribotų riziką, susijusią su nepilnamečiais, kurie yra socialinių tinklų svetainių nariai. Nuomonėje kalbama apie socialinių tinklų svetainių naudotojų teises bei asmenų, kurie nėra nariai, pranešimą šiuo klausimu. Šios teisės apima teisę į neteisingos informacijos ištaisymą ir teisę susipažinti su joje saugoma informacija. Vėlgi, nuomonėje pabrėžiama, kad socialinių tinklų svetainių pagrindinis puslapis turėtų aiškiai nurodyti skundų nagrinėjimo tarnybą, kurioje būtų nagrinėjami duomenų apsaugos pažeidimų klausimai ir skundai, kuriuos pateikia tiek nariai, tiek ne nariai. Beje, nors 29 str. duomenų apsaugos

[50] SCAIFE, Laura. *Handbook of Social Media and the law.* Informa Law from Routledge; 1 edition, 2015, p. 277.
[51] ES 29 str. darbo grupė. *2009 m. birželio 12 d. Nuomonė 5/2009 dėl socialinių tinklų,* Nr. WP 163.
[52] Ibid.

darbo grupės pateikiama nuomonė nėra teisiškai įpareigojanti, svarbu pabrėžti jos akivaizdų indelį kuriant aiškesnį socialinių tinklų reguliavimą.

Pastebėjus milžinišką informacijos vertę, nustačius kylančias grėsmes duomenų saugumui, visa tai paskatino priimti Bendrąjį duomenų apsaugos reglamentą, siekiant vieningo duomenų apsaugos teisės reguliavimo. 2016 m. buvo priimtas Bendrasis duomenų apsaugos reglamentas, kaip tiesioginio taikymo aktas, kuris 2018 m. suvienodino ES valstybių narių duomenų apsaugos teisę. Bendrasis duomenų apsaugos reglamentas paremtas iš esmės tais pačiais pagrindais, kaip ankstesnis duomenų apsaugos teisės reguliavimas ES[53]. Bendrasis duomenų apsaugos reglamentas yra taikomas viso pasaulio organizacijoms, kreipiančioms veiklą į ES. Kitaip tariant, išplečiama teritorinė taikymo sritis. Be to, Bendrasis duomenų apsaugos reglamentas įtvirtina atskaitomybės principą, kuriuo siekiama suteikti didesnę atsakomybę duomenų valdytojams. Taip pat, Bendruoju duomenų apsaugos reglamentu griežtinami sutikimo, kaip vieno iš alternatyvių duomenų tvarkymo pagrindų, reikalavimai. Reguliavimu įpareigojama užtikrinti duomenų subjektų teises, tokiu atveju yra įtvirtinama nauja duomenų subjektų teisė – teisė į duomenų perkėlimą. Bendrajame duomenų apsaugos reglamente nustatyta pareiga paskirti duomenų apsaugos pareigūną[54]. Be to, naujasis reguliavimas įtvirtiną naują bendro pobūdžio pareigą duomenų valdytojams nedelsiant ir, jei įmanoma, per 72 valandas pranešti priežiūros institucijai apie saugumo pažeidimą, nebent pažeidimas neturėtų kelti pavojaus asmenims. Be to, Bendrajame duomenų apsaugos reglamente detaliai nustatyti atvejai ir konkrečios priemonės, leidžiančios duomenų valdytojams perduoti duomenis į trečiąsias valstybes arba tarptautinėms organizacijoms[55]. Nors Reglamente nėra užsimenama apie duomenų apsaugą socialiniuose tinkluose, tačiau įtvirtintos naujovės turėtų priversti socialinių tinklų bendroves pritaikyti Bendrojo duomenų apsaugos reglamento reikalavimus ir užtikrinti teisėtus duomenų tvarkymo būdus. Be to, iki įsigaliojant Bendrajam duomenų apsaugos reglamentui, socialiniai tinklai asmens duomenis galėdavo rinkti perteklinai, vartotojams nebuvo suteikiama galimybė išsitrinti paskyras, bei nebuvo įgyvendinta teisė prieiti prie savo duomenų, juos taisyti, perkelti ir ištrinti.

[53] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. VĮ Registrų centras, Vilnius, 2019, p. 329.
[54] 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.
[55] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei, Teisė, 2017, t. 103

2. BENDROJO DUOMENŲ APSAUGOS REGLAMENTO TAIKYMAS SOCIALINIUOSE TINKLUOSE

2.1 Duomenų samprata

Naudojantis elektroninėmis ryšio priemonėmis, internete apdorojama vis daugiau duomenų, susijusių su konkrečiu asmeniu. Apie asmenį galima surinkti informaciją, kuri gali apibūdinti jo įpročius, pomėgius. Neteisėtai renkant ir netinkamai naudojant šiuos duomenis gali kilti didelė grėsmė tokių asmenų privatumui[56]. Duomenų apsaugos teisės materialinę taikymo sritį pirmiausia lemia asmens duomenų samprata. Duomenų apsaugos teisės reikalavimai taikomi tik nustačius, kad konkreti informacija patenka į duomenų apibrėžtį. Bendrasis duomenų apsaugos reglamentas taikomas ne bet kokios informacijos, bet asmens duomenų tvarkymui[57].

Kalbant apie privačią informaciją ir asmens duomenis svarbu atkreipti dėmesį, jog tai nėra tapačios sąvokos. Žinoma, asmens duomenų apsauga yra neatskiriama nuo privataus gyvenimo apsaugos. Asmens duomenys yra vienas iš asmens privataus gyvenimo elementų, o su šių duomenų rinkimu ir naudojimu susijusi veikla turi įtaką asmens privačiam gyvenimui. Garantuojant asmens teisę į privatų gyvenimą, kartu garantuojama ir jo asmens duomenų apsauga, o kita vertus – užtikrinant asmens duomenų apsaugą yra saugomas ir asmens privatus gyvenimas[58]. Kitaip tariant, teisė į duomenų apsaugą išsivystė iš teisės į privatų gyvenimą, kuri yra fundamentali žmogaus teisė. Duomenų apsaugos mokslininkas A. Westin apibrėžė asmens teisę į privatų gyvenimą kaip galimybę kontroliuoti, taisyti, valdyti ir ištrinti informaciją apie save ir kitus, ir nuspręsti kada, kaip, ir kokia apimtimi ta informacija galėtų būti pasiekiama kitiems asmenims. Be to, ši privatumo sąvoka pagrindė pamatus ir velesnei moderniai privatumo koncepcijai[59]. Mokslinio pripažinimo sulaukusi asmens teisė į privatumą, pamažu buvo įtvirtinta tarptautiniuose teisės aktuose. Pirmiausia, priimta Visuotinė žmogaus teisių deklaracija, kurios 12 straipsnyje teigiama, kad niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą, kėsinimosi į jo garbę ir reputaciją,

[56] ŠTITILIS, D. et al. Interneto ir technologijų teisė: vadovėlis. Mykolo Romerio universitetas. – Vilnius: Registrų centras, 2016. p. 328.
[57] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius, 2019, p. 91.
[58] PETRAITYTĖ, I. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2017, t. 80, p. 165.
[59] WESTIN, Alan. Privacy and Freedom. *Washington and Lee Law Review* 1, 20 (1668): p. 166-170.

kad kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsinimosi[60]. Kitas svarbus tarptautinis dokumentas, užtikrinantis asmens privatumo apsaugą – Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija, kurios 8 straipsnis iš esmės skirtas apsaugoti individus nuo neteisėto valstybių kišimosi į jų asmeninę erdvę[61]. Šio straipsnio turinys plačiau atskleidžiamas Europos Žmogaus Teisių Teismo sprendimuose. Teismas yra nustatęs, kad privataus gyvenimo sąvoka apima asmenybės raidą asmens santykiuose su kitais asmenimis, asmens fizinį ar moralinį vientisumą, seksualinę orientaciją ir lytinį gyvenimą, informaciją apie asmenį[62]. Tačiau nors ir asmens duomenys stipriai susiję su privačia informacija, visgi privatumo koncepcija plėtojosi kita linkme. Reikėtų paminėti, jog asmens duomenų apsauga sudaro tik vieną iš keturių privatumo elementų. Nepaisant to, asmens duomenų apsauga yra labai svarbi privatumo kategorija, siejama su asmens teise kontroliuoti informacijos apie save tvarkymą[63].

Siekiant išsamiai atskleisti duomenų apsaugos veikimą socialiniuose tinkluose, svarbu išnagrinėti ir šios teisės objekto, t.y. asmens duomenų, sampratą. Visų pirma, reikia pažymėti, jog asmens duomenys – tai teisinė kategorija, įtvirtinta Bendrajame duomenų apsaugos reglamente, kuriame asmens duomenimis laikoma bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius[64]. Taigi, asmens duomenų sąvoka apima bet kokios formos, bet kokio turinio informaciją nepriklausomai nuo jos šaltinio ir valdytojo, jeigu tik šią informaciją galima susieti su konkrečiu asmeniu[65].

Svarbu paminėti, jog įsigaliojus Bendrajam duomenų apsaugos reglamentui, asmens duomenų sąvoka pakito minimaliai – atsirado kelios modernios kategorijos

[60] 1948 m. gruodžio 10 d. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006-06-17, Nr. 68-2497.
[61] 1950 m. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. *Valstybės žinios*, 1995-05-16, Nr. 40-987.
[62] Europos žmogaus teisių teismo 1992 m. gruodžio 16 d. sprendimas *Niemietz v. Germany,* Nr. 13710/88*;* Europos žmogaus teisių teismo 1985 m. kovo 26 d. sprendimas *X and Y v. Netherlands,* Nr. 8978/80; Europos žmogaus teisių teismo 2000 m. gegužės 4 d. sprendimas 28341/95 *Rotaru v. Romania,* Nr. 28341/95.
[63] ŠTITILIS, D. et al. Interneto ir technologijų teisė: vadovėlis. Mykolo Romerio universitetas. – Vilnius: Registrų centras, 2016. p. 328.
[64] 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.
[65] PETRAITYTĖ, I. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2017, t. 80, p. 53.

apibūdinančios asmens duomenų sampratą, tai buvimo vietos duomenys, interneto identifikatoriai bei genetiniai duomenys. Beje, šios kategorijos gali pasirodyti iššūkiu organizacijoms, siekiant laikytis reglamento reikalavimų. Pavyzdžiui, socialinių tinklų svetainėms daugelio rūšių slapukai (angl. *cookies*) tampa asmens duomenimis pagal Bendrąjį duomenų apsaugos reglamentą, kadangi slapukai yra laikomi interneto identifikatoriais. Be to, įmonės, kurios renka asmens buvimo vietą, taip pat privalo laikytis Bendrojo duomenų apsaugos reglamento, kadangi nuo šiol asmens buvimo vieta taip pat priskiriama prie asmens duomenų.

Akivaizdu, jog asmens duomenų sąvoka yra ganėtinai plati ir lanksti, todėl daugeliu atveju gali kilti neaiškumų, kokios pozicijos laikytis, ar asmenims taikoma duomenų apsaugos teisė ir, ar duomenų valdytojai turėtų laikytis Bendrojo duomenų apsaugos reglamento įpareigojimų. Nagrinėjant asmens duomenų sąvoką, ES 29 straipsnio duomenų apsaugos darbo grupės (toliau – 29 str. darbo grupė) nuomonėje 4/2007 dėl asmens duomenų sąvokos išskyrė keturis svarbius elementus:

- Tai bet kuri informacija;
- Susijusi su;
- Tapatybė yra nustatyta arba gali būti nustatyta;
- Fizinis asmuo (duomenų subjektas)[66].

Svarbu paminėti, jog platus sąvokos turinys yra siekiant apimti visą galimą informaciją susijusią su asmeniu, jog būtų užtikrinama tinkama asmens duomenų apsauga[67]. Informacija gali būti objektyvi, subjektyvi, jai gali būti priskiriama nuomonė bei vertinimai. Be kita ko, kad informacija būtų pripažinta asmens duomenimis, ji neprivalo būti teisinga ar įrodyta[68]. Internete informaciją būtina vertinti kaip objektą, kuris neturi baigtinės formos, nėra fiksuotas turinio, vietos ar laiko požiūriu. Internete skirtingi informacijos elementai egzistuoja skirtingose vietose, juos tvarko skirtingi subjektai, dalis tokių elementų yra paviešintų teisėtai, dalis – į internetą patekusių neteisėtai[69].

Informacijos sąsajumo su asmeniu padarinys yra tas, kad kiekviena su asmeniu susijusi informacija gali identifikuoti asmenį neatsižvelgiant į tai kas, kokiu tikslu ir

[66] ES 29 str. darbo grupės 2007 m. birželio 20 d. nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 6. [interaktyvus; Žiūrėta 2019 m. lapkričio 10 d.]. Prieiga per internetą: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.
[67] *Ibid.*, p. 4.
[68] ES 29 str. darbo grupės 2007 m. birželio 20 d. nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 6. [interaktyvus. Žiūrėta 2019 m. lapkričio 10 d.]. Prieiga per internetą: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.
[69] CIVILKA, M. ir ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje, Teisė, 96, 2015, p. 126-148.

kokias priemones pasitelkdamas, vertina tą informaciją[70]. Informacija laikoma susijusia su asmeniu tada, kai ji yra apie tą asmenį. Duomenys yra susiję su asmeniu, jeigu jie nurodo asmens tapatybę, ypatybes ar elgesį arba, jei tokia informacija naudojama siekiant nustatyti, kaip elgiamasi su tuo asmeniu, arba kaip jis vertinamas, arba daryti jam poveikį[71].

Asmens tapatybės nustatymo galimybė yra ypač svarbus elementas. Kai kalbame apie asmens duomenis, neišvengiamai susiduriama su sąvoka „asmens tapatybė". Asmens duomenys, kuriems suteikti pseudonimai ir, kurie galėtų būti priskirti fiziniam asmeniui, pasinaudojus papildoma informacija, turėtų būti laikomi informacija apie fizinį asmenį, kurio tapatybė gali būti nustatyta. Akcentuotini du kriterijai – tiesioginis ir netiesioginis asmens tapatybės nustatymas, tai leidžia apimti daug duomenų, kurie iš pirmo žvilgsnio gali atrodyti turintys menką ryšį su konkrečiu asmeniu. Duomenys gali būti asmeniniai netgi tada, jeigu juos pasitelkus asmuo gali būti identifikuotas tik turint kitų duomenų kombinaciją – pagalbinius duomenis. Kita vertus, svarbu, kad asmens tapatybės nustatymas turi būti įmanomas be neprotingų laiko, darbo ir kitų sąnaudų. Kad būtų galima nuspręsti, ar galima nustatyti asmens tapatybę, reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo, asmens tapatybei nustatyti[72].

Be to, duomenų apsaugos principai neturėtų būti taikomi anonimiškai informacijai, t. y. informacijai, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta. Todėl Bendrasis duomenų apsaugos reglamentas netaikomas tokios anonimiškos informacijos tvarkymui, įskaitant statistiniais ar tyrimų tikslais[73].

Padidėjęs vartotojų skaičius, naudojantis elektroniniais įrenginiais, sudarė sąlygas vartotojams internete palikti ir aptikti galybę duomenų, nebūtinai atskleidžiančių jų vardus ir pavardes, tačiau unikaliai nusakančių jų asmeniui būdingas savybes ar požymius. Tapatumas virtualioje erdvėje pasižymi tuo, kad svarbiau yra išskirti asmenį iš asmenų grupės, nei pasakyti, koks yra to asmens tikslus vardas ar pavardė. Šiam tikslui svarbūs kiti duomenys: interneto protokolo (IP) adresas, prisijungimo prie įvairių profilių

[70] FLORIDI, Luciano. *Information a very short introduction*. Oxford University Press, 2010, p. 1.
[71] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Vilnius, 2019, p. 93.
[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, p. 1-88.
[73] *Ibid*.

dažnis, perkamų prekių asortimentas, reklamų peržiūros, lankomi tinklalapiai, juose praleidžiamas laikas ir t.t.[74].

Fizinio asmens elementas reiškia, jog Bendrojo duomenų apsaugos reglamento taisyklėse numatyta apsauga yra taikoma tik fiziniams asmenims, tvarkant jų asmens duomenis, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą. Be to, svarbu paminėti, jog asmens duomenų apsauga yra susijusi tik su gyvais asmenimis.[75]

Bendrasis duomenų apsaugos reglamentas, remiantis skaidrumo principu, įpareigoja duomenų valdytojus duomenų subjektams, fiziniams asmenims pateikti aiškią informaciją, kaip su jais susiję asmens duomenys yra renkami ir naudojami, kaip su jais susipažįstama arba kaip kitaip jie yra tvarkomi, taip pat kokios apimties tie asmens duomenys yra ar bus tvarkomi[76].

Siekiant nustatyti, kokie asmens duomenys yra renkami socialiniuose tinkluose, svarbu išanalizuoti socialinių tinklų privatumo politikas. Šiame darbe pasirinkta analizuoti socialinio tinklo Facebook privatumo politiką, ne tik dėl to, kad tai populiariausias ir daugiausiai vartotojų turintis socialinis tinklas, bei kuriam priklauso dar du kiti populiarūs socialiniai tinklai – „Instagram" ir „Whatsapp", tačiau ir dėl pastaruoju metu šį socialinį tinklą krečiančių skandalų, susijusių su duomenų apsauga.

„Facebook" renka visus duomenis, susijusius su bet kuriuo „Facebook" produkto naudojimu. Tai gali būti ne tik informacija, kuria aktyviai dalinasi vartotojai, tačiau tai taip pat apima duomenis, kuriuos naršyklė ar įrenginys automatiškai perduoda į „Facebook", kai tinklas yra naudojamas. Tai apima, pavyzdžiui, informaciją apie žmones, puslapius ar grupes, prie kurių vartotojai yra prisijungę ar su kuriais sąveikauja. Taip pat renkama kontaktinė informacija, kurią vartotojas įkelia, sinchronizuoja arba importuoja iš įrenginio. „Facebook" renka informaciją apie tai, kokį turinį vartotojas mato ir kaip jie sąveikauja su šiuo turiniu ar kokias operacijas jie vykdo. „Facebook" nurodo, kokią informaciją jis renka iš naudojamų kompiuterių, telefonų, prijungtų televizorių ir kitų prie interneto prijungtų įrenginių, jei jie integruoti su „Facebook" produktais. „Facebook" sujungia šią informaciją apie visus vartotojo naudojamus įrenginius ir paslaugas. Tai apima daugybę atributų (operacinę sistemą, aparatinę ir programinę įrangą, naršyklės tipą ir kt.), informaciją apie operacijas ir įrenginyje atliktas veiklas, identifikatorius (įrenginio

[74] CIVILKA, M. ir ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje, Teisė, 96, 2015, p. 126-148.

[75]ES 29 str. darbo grupės 2007 m. birželio 20 d. nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 24. [interaktyvus; Žiūrėta 2019 m. lapkričio 10 d.]. Prieiga per internetą: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.

[76] 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.

ID ir kitus identifikatorius, pavyzdžiui, iš žaidimų, programėlių, paskyrų), įrenginio signalų (Bluetooth, WLAN signalų ir kt.), duomenys iš įrenginio nustatymų (pavyzdžiui, informacija, kurią galima gauti naudojantis įjungtais įrenginio nustatymais, tokiais kaip prieiga prie vartotojo GPS vietos, fotoaparato ar nuotraukų ir t.t.), tinklas ir ryšiai (informacija, tokia kaip vartotojo mobiliojo telefono pavadinimas, paslaugų operatorius arba IP adresas, mobiliojo telefono numeris, taip pat vartotojo įrenginyje saugomų slapukų duomenys, įskaitant slapukų duomenis susijusius su ,,Facebook" ir ,,Instagram" slapukų politika. Remiantis privatumo politika, ,,Facebook" taip pat gali rinkti duomenis iš reklamuotojų, programėlių kūrėjų ir leidėjų (vadinamų partneriais), kurie naudojasi ,,Facebook" verslo įrankiais, apie vartotojų veiklą ne ,,Facebook". ,,Facebook" savo privatumo politikoje nurodo, kad partneriai jam teikia informaciją apie vartotojų veiklą už socialinio tinklo ribų, įskaitant informaciją apie vartotojo įrenginį, lankomas internetines svetaines, darytus pirkimus, matomus skelbimus ir tai, kaip naudojamasi jų paslaugomis, nesvarbu, ar vartotojas turi ,,Facebook" paskyrą, ar yra prisijungęs prie ,,Facebook". Socialinis tinklas taip pat registruoja vartotojo veiksmus prisijungus ar būnant neprisijungus, taip pat pirkimus iš trečiųjų šalių duomenų teikėjų[77].

Tačiau negalima tikėtis, kad iš ,,Facebook" surenkamų duomenų, nebūtų įtraukiami asmens duomenys iš specialiųjų kategorijų pagal Bendrąjį duomenų apsaugos reglamento 9 straipsnio 1 dalį. Reglamentas išlaiko draudimą, anksčiau numatytą Direktyvoje 95/46/EB, tvarkyti jautrius (Reglamente – specialių kategorijų) duomenis, nebent egzistuoja viena iš išimčių, numatytų Reglamento 9 straipsnio 2 dalyje. Draudžiama tvarkyti asmens duomenis, atskleidžiančius rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, ar narystę profesinėse sąjungose, taip pat tvarkyti genetinius duomenis, biometrinius duomenis, siekiant konkrečiai nustatyti fizinio asmens tapatybę, sveikatos duomenis arba duomenis apie fizinio asmens lytinį gyvenimą ir lytinę orientaciją. Prie jautrių duomenų papildomai priskiriami genetiniai ir biometriniai duomenys. Tai tokio tipo duomenys, kurie gali sukelti didesnę riziką asmens pagrindinėms teisėms ir laisvėms.

Itin jautrūs duomenys gali būti skelbiami internete, tik gavus aiškų duomenų subjekto sutikimą arba, jei duomenų subjektas savo noriu, itin jautrius duomenis pateikė viešai. Tačiau socialiniai tinklai, kaip duomenų valdytojai, negali tvarkyti socialinių tinklų vartotojų itin jautrių duomenų be vartotojų aiškaus sutikimo. Jei į socialinio tinklo

[77] Facebook privatumo politika. [Interaktyvus. Žiūrėta 2019 m. rugsėjo 12 d.] Prieiga per internetą: <https://www.facebook.com/full_data_use_policy>.

anketos klausimus įtraukiami ir klausimai apie itin jautrius duomenis, socialiniai tinklai turi aiškiai nurodyti, kad atsakyti į juos yra neprivaloma[78].

Taigi, duomenų profiliavimas gali sudaryti specialių kategorijų duomenų profilius, vien remiantis išvadomis iš duomenų, kurie nėra specialiųjų kategorijų duomenys, bet tokiais tampa, kai derinami su kitais duomenimis. Pavyzdžiui, gali būti įmanoma padaryti išvadą apie asmens sveikatos būklę iš maisto pirkinių įrašų kartu su duomenimis apie maisto kokybę ir energijos kiekį[79]. Vieno tyrimo metu buvo nustatyta, kad vien iš „Facebook" vartotojų funkcijos „Patinka" paspaudimų ir ribotos informacijos apie vartotoją, tyrėjams pavyko 88 proc. tikslumu numatyti vyro seksualinę orientaciją; 95 proc. tikslumu pavyko nustatyti vartotojo etninę kilmę; nustatyti ar vartotojas buvo krikščionis, ar musulmonas pavyko 82 proc. tikslumu[80]. Atsižvelgiant į „Facebook" privatumo politiką, negalima manyti, kad informacija, kurią kaupia „Facebook" yra tik informacija, iš kurios gali būti gaunami jautrūs duomenys, ir kad to nepakanka, kad ji būtų priskiriama prie jautrios informacijos. Tuolab, kad kai informacija apie aplankytą puslapį, priskiriama „Facebook" vartotojo anketai, jautrūs duomenys privalo būti laikomi specialių kategorijų duomenimis, kadangi jie akivaizdžiai priskirti fiziniam asmeniui.

Pagal Bendrojo duomenų apsaugos reglamento 9 straipsnio 1 dalies formuluotę, norint klasifikuoti kaip specialių kategorijų duomenis, pakanka, kad duomenys atskleistų tam tikrą savybę. Tai nereiškia, kad patys duomenys turi atskleisti charakteristiką. Pakanka, kad duomenų turinys, bent jau netiesiogiai, atskleistų minėtą požymį vidutiniam, objektyviam trečiajam asmeniui[81]. Duomenų rinkimas trečiųjų šalių svetainėse ir programose gali lengvai generuoti duomenis apie rasinę ir etninę kilmę, politines nuomones ar ideologinius įsitikinimus. „Facebook" pasitelkdamas „Facebook" verslo įrankius, tokius kaip API, „Facebook" Login, „Facebook" Pixel, renka duomenis, identifikuojančius konkrečias vartotojo savybes. Pavyzdžiui, programėlė „Tinder" siūlo prisijungti per „Facebook" Login įrankį, taip pat daugybė medicinių įstaigų puslapiai turi integruotą mygtuką „Bendrinti/Dalintis Facebook". Vienas aktualiausių pavyzdžių, naujausiame „The Wallstreet Journal" tyrime, buvo nustatyta, jog kelios populiariausios

[78] ES 29 str. darbo grupės 2019 m. birželio 12 d. Nuomonė Nr. 5/2009 dėl internetinių socialinių tinklų Nr. WP163. [interaktyvus; žiūrėta 2019 m. Spalio 20 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>.

[79] ES 29 str. darbo grupės 2017 m. spalio 3 d. Gairės dėl automatizuoto spendimų priėmimo ir profiliavimo Reglamento (ES) 2016/679 tikslais Nr. WP251 [interaktyvus. Žiūrėta 2019 m. rugsėjo 12 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053.

[80] KOSINSKI, Michael., STILWELL, David., GRAEPEL, Thore. Private traits and attributes are predictable from digital records of human behavior. Proceedings of the National Academy of Sciences of the United States of America. [Interaktyvus. Žiūrėta 2019 m. spalio 23 d.]. Prieiga per internetą: https://www.pnas.org/content/pnas/110/15/5802.full.pdf.

[81] EHMANN, Eugen., SELMAYR, Martin. *Does Article 9 GDPR rule out the permissibillity of processing with big data?*, ZD 2017, p. 305.

išmaniųjų telefonų programos, socialiniui tinklui „Facebook", perduoda jautrią asmeninę informaciją apie savo vartotojus, įskaitant kraujospūdį, svorį, neštumo skaičiavimo ciklus, be vartotojo žinios bei jo sutikimo. Teigiama, kad ne mažiau kaip 11 programų tokius duomenis perdavė „Facebook". Visos programėlės apima „Facebook" kodą, leidžiantį jos kūrėjams stebėti, kaip yra naudojamos programėles, su tikslu pasiūlyti tinkamą reklamą[82]. Tai leidžia socialinam tinklui kurti išsamius profilius apie vartotoją, naudojant ir neskelbtinus vartotojo duomenis.

Nemažai tyrimų parodė, jog pasitelkus algoritmus, iš „Facebook" bei „Twitter" asmeninių paskyrų, kuriuose asmuo palieka internetinius duomenis, visai nesudėtinga nustatyti asmens tikslius duomenis: amžių, lytį, ar asmuo linkęs būti nervingu, ar lengvai įsitempusiu, asmens impulsyvumą, ar politines pažiūras. Kita vertus, algoritmo gebėjimas daryti išvadas apie asmenis, rodo, kaip lengva kiekvienam, kuris seka asmenų veiklą internete, įgyti įžvalgų apie asmenybes ir galbūt pažeisti privatumą. Be to, psichologinės išvados apie asmenis gali būti panaudotos manipuliuoti[83].

Taip pat, 2015 m. Davido Stillwello ir Youyou Wu iš Kembridžo universiteto ir Michalo Kosinskio iš Stanfordo universiteto atliktas tyrimas parodė, kad algoritmai gali įvertinti, psichologų vadinamą žmogaus asmenybės tyrimo prieigą (asmenybės bruožų teorija), vien tik išnagrinėdami „Facebook" vartotojo funkcijos „Patinka" paspaudimus. Šie matmenys - atvirumas patirčiai, sąmoningumas, ekstraversija, sutariamumas ir emocinis stabilumas - yra laikomi pagrindiniais asmenybės matmenimis. Todėl atskleidus šias savybes, nesunku apibūdinti, kas yra tie analizuojami žmonės. Tyrimo metu, „Facebook" varototojai užpildė asmenybės anketas, kurių metu mokslininkams iš anksto buvo žinomi penki asmenybės aspektai apie tyrime dalyvaujančius asmenis. Tuomet mokslininkų sukurtas algoritmas išanalizavo tyrime dalyvavusių „Facebook" vartotojų funkcijos „Patinka" paspaudimus. Buvo padaryta išvada, jog algoritmas turi galimybę gana greitai atpažinti asmenį ir netgi pažinti jį geriau nei bendradarbis, šeimos narys ar sutuoktinis[84]. Būtent šio tyrimo kontekste, svarbu paminėti „Cambridge Analytica" skandalą. Funkcijos „Patinka" paspaudimų tyrimai įkvėpė duomenų analizės mokslininką surinkti ir pasidalyti iki 87 milijonų Facebook naudotojų duomenimis be jų sutikimo ir

[82] SCHECHNER, Sam. You Give Apps Sensitive Personal Information. Then They Tell Facebook. [interaktyvus. Žiūrėta 2019-02-28]. Prieiga per internetą: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636

[83] AZUCAR, Danny. et al. Predicting the Big 5 Personality Traits from Digital Footprints on Social Media: A Meta-Analysis. *Personality and Individual Differences*, Vol. 124, 2018, p 150–159.

[84] YOUYOU, Wu. et al. Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans. *Proceedings of the National Academy of Sciences USA*, Vol. 112, No. 4, 2015, p. 1036–1040. [interaktyvus. Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: < http://www.richardbenjamintrust.co.uk/uploads/finalreports/2013/DStillwell.pdf>.

žinios su „Cambridge Analytica" politinės strategijos ir reklamos konsultantais, kurie teikė paslaugas JAV prezidento Donaldo Trumpo rinkimų kampanijai[85].

2.2. Duomenų valdytojai

Pagal Bendrojo duomenų apsaugos reglamento 4 straipsnio 7 punktą, asmens duomenų valdytojas reiškia fizinį ar juridinį asmenį, valstybės valdžios instituciją, agentūrą ar kitą įstaigą, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones[86]. Taigi, apibrėžimas akcentuoja keturis momentus. Pirma, jis numato galimybę, kad vienos asmens duomenų tvarkymo operacijos metu gali dalyvauti daugiau nei vienas asmens duomenų valdytojas. Antra, asmens duomenų valdytojas nebūtinai turi turėti, valdyti asmens duomenis. Trečia, kintant duomenų tvarkymo operacijoms, gali kisti pati duomenų valdytojo samprata. Ketvirta, apsprendžiantysis veiksnys, tam tikrą subjektą pripažįstant duomenų valdytoju, yra ne formalus duomenų tvarkymo operacijų kontrolės atsakomybės paskirstymas, bet faktinis tos kontrolės vykdymas[87].

Pagal duomenų apsaugos teisę, duomenų valdytojui tenka pagrindinė atsakomybė – įgyvendinti visus nustatytus reikalavimus. Remiantis atskaitomybės principu, duomenų valdytojas yra atsakingas už tai, kad būtų laikomasi duomenų apsaugos teisės reikalavimų, ir turėtų sugebėti įrodyti, kad jų laikomasi[88].

Bendruoju duomenų apsaugos reglamentu galima išskirti kelias duomenų apsaugos naujoves, kurios perbraižo duomenų valdytojų atsakomybės, už atitiktį duomenų apsaugos standartams, ribas[89]. Tai griežtinami sutikimo, kaip vieno iš alternatyvių duomenų tvarkymo pagrindų, reikalavimai. Duomenų valdytojas turi turėti įrodyti, jog duomenų subjektas davė sutikimą, kad būtų tvarkomi jo asmens duomenys. Apsaugos priemonėmis turi būti užtikrinta, kad duomenų subjektas suvoktų, kad jis duoda sutikimą ir dėl ko jis jį duoda. Kad sutikimas būtų grindžiamas informacija, duomenų subjektas turėtų žinoti bent duomenų valdytojo tapatybę ir asmens duomenų tvarkymo

[85] The Guardian. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 2018 m. kovo 17 d. [Interaktyvus. Žiūrėta 2019 m. rugsėjo 10 d.]. Prieiga per internetą: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
[86] 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.
[87] CIVILKA, Mindaugas., et al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004, p. 102.
[88] 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.
[89] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei, Teisė, 2017, t. 103, p. 47.

tikslus. Be to, sutikimas neturėtų būti laikomas duotas laisva valia, jei duomenų subjektas faktiškai neturi laisvo pasirinkimo ar negali atsisakyti sutikti arba sutikimo atšaukti[90].

Taip pat, pasak J. Zaleskio, reiškmingą poveikį duomenų apsaugos teisei turėtų padaryti atskaitomybės principo, pareigos atlikti poveikio vertinimą, konsultacijos su priežiūros institucija, duomenų apsaugos pareigūno paskyrimo, pranešimo priežiūros institucijai ir išankstinės patikros procedūros panaikinimo, naujovių visuma[91].

Bendroju duomenų apsaugos reglamentu, kaip tai nurodyta 24 straipsnyje, duomenų valdytojui suteikiamas savarankiškumas pačiam atsižvelgti į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, įvertinti kylančius pavojus asmenims ir nustatyti reikalingumą kreiptis į priežiūros insitituciją, kitaip tariant, atlikti poveikio duomenų apsaugai vertinimą. Duomenų valdytojas atlikęs poveikio duomenų apsaugai vertinimą, turi konstultuotis su priežiūros institucija, jeigu poveikio duomenų apsaugai vertinime nurodyta, kad tvarkant duomenis kiltų didelis pavojus, jei duomenų valdytojas nesiimtų priemonių pavojui sumažinti, prieš pradėdamas tvarkyti duomenis[92]. Šiuo atveju, iškyla klausimas, kokiais konkrečiais atvejais duomenų valdytojas privalo atlikti poveikio duomenų apsaugai vertinimą. Bendrojo duomenų apsaugos reglamento 35 straipsnio 2 dalyje yra numatytas poveikio duomenų apsaugai reikalingumas bent šiais trim atvejais:

- Atliekant sistemingą ir išsamų su fiziniais asmenimis susijusių asmeninių aspektų vertinimą, įskaitant profiliavimą;
- Tvarkant didelio kiekio specialiųjų kategorijų duomenų arba duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas;
- Sistemingai stebint viešąsias erdves dideliu mastu.

Šiuo aspektu 29 straipsnio darbo grupė poveikio duomenų apsaugai vertinimo gairėse numato daugiau požymių, kuriais remiantis duomenų valdytojas turėtų atlikti poveikio duomenų apsaugai vertinimą, tačiau daugiausiai neaiškumų kyla siekiant nustatyti, kada duomenys yra tvarkomi dideliu mastu[93]. Bendrasis duomenų apsaugos reglamentas neapibrėžia duomenų tvarkymo dideliu mastu, tačiau preambulės 91 dalyje,

[90] 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.

[91] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei, Teisė, 2017, t. 103, p. 50.

[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 5 4, p. 1-88.

[93] ES 29 str. darbo grupė. 2017 m. spalio 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, WP 248 rev. 01, p. 9-11.

numatytos tam tikros užuominos. Be to, 29 straipsnio darbo grupė, pateikdama rekomendaciją, nustatant ar duomenų tvarkymas yra atliekamas dideliu mastu, taip pat apsiribojo ganėtinai abstrakčiu vertinimu. Ji nurodo, kad duomenų tvarkymas dideliu mastu yra esant dideliam subjektų skaičiui, dideliai duomenų apimčiai, atsižvelgiant į duomenų tvarkymo veiklos trukmę ar skirtingų duomenų įvairovę, duomenų apimtį bei geografinį duomenų tvarkymo mastą[94]. Taip pat nėra nurodyta, ar nustatant duomenų tvarkymą dideliu mastu reikia vadovautis kriterijų visuma, ar pakanka vieno jų.

Pasitaiko atvejų, kai įvairiose duomenų tvarkymo operacijose ar operacijų cikluose dalyvauja skirtingi subjektai. Šios operacijos gali vykti vienu metu arba keliais etapais. Du ar daugiau duomenų valdytojų, kartu nustatančių duomenų valdymo tikslus ir priemones, laikomi bendrais duomenų valdytojais[95].

Bendrų duomenų valdytojų institutu siekiama užtikrinti veiksmingą ir visapusišką atitinkamų asmenų apsaugą, todėl bendros atsakomybės buvimas nebūtinai reiškia, kad įvairių su tuo pačiu asmens duomenų tvarkymu susijusių asmenų atsakomybė yra lygiavertė. Atvirkščiai, šie asmenys gali dalyvauti tvarkant duomenis skirtinguose etapuose ir skirtingu mastu, todėl kiekvieno jų atsakomybės lygis turi būti įvertintas atsižvelgiant į visas reikšmingas konkretaus atvejo aplinkybes. Be to, tai, kad keli asmenys gali būti atsakingi už tą patį tvarkymą, nereiškia, kad kiekvienas iš jų turi turėti galimybę susipažinti su atitinkamais asmens duomenimis[96].

Duomenų valdytojo pozicija socialinių tinklų kontekste gali skirtis, galimi keli skirtingi atvejai, kuomet duomenų valdytojas socialiuose tinkluose bus laikomas vis kitas asmuo. Pirma, socialinio tinklo teikėjas yra laikomas duomenų valdytoju, nes jis apibrėžia socialinių tinklų vartotojų asmens duomenų tvarkymo tikslus ir priemones bei pagrindines su vartotojų valdymu susijusias paslaugas (pvz., profilio susikūrimas bei jo ištrynimas). Jie taip pat nustato, kaip vartotojo duomenys gali būti naudojami reklamos ar rinkodaros tikslais, įskaitant trečiųjų šalių teikiamą reklamą. Antra, be pagrindinės socialinių tinklų paslaugos, trečiosios šalys gali pasiūlyti įdiegti papildomas programas, pavyzdžiui, žaidimus ar paslaugą, leidžiančią vartotojams siųsti virtualias dovanas. Tokiu atveju programos teikėjai nustato, kokie tikslai ir kaip asmens duomenys naudojami

[94] ES 29 str. darbo grupė. 2017 m. spalio 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, WP 248 rev. 01, p. 9-11

[95] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. VĮ Registrų centras, Vilnius, 2019, p. 59.

[96] ES Teisingumo Teismo 2018 m. liepos 10 d. sprendimas byloje C25/17 *Jehovan todistajat*, EU:C:2018:551. [Interaktyvus. Žiūrėta 2019 m. spalio 12 d.]. Prieiga per internetą: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=203822&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=2239521>.

programoje. Jie atsiunčia duomenis per programavimo sąsają (API), naudodami vartotojo pateiktus prisijungimus ir slaptažodžius. Tokiu būdu programos teikėjas taip pat yra asmens duomenų valdytojas. Galiausiai, socialinių tinklų svetainių vartotojai taip pat gali būti laikomi duomenų valdytojais. Tai tokie atvejai, kai socialinių tinklų vartotojas veikia įmonės ar asociacijos vardu, arba naudoja socialinius tinklus, dažniausiai, kaip platformą komerciniams, politiniams ar labdaros tikslams pasiekti. Tokiais atvejais vartotojas prisiima duomenų valdytojo atsakomybes, kadangi atskleidžia asmens duomenis kitam duomenų valdytojui (socialiniam tinklui) ir tretiesiems asmenims (kitiems socialinių tinklų vartotojams arba net kitiems duomenų valdytojams, kurie turi prieigą prie tų duomenų). Be to, paprastai prieiga prie duomenų (paskyros duomenų, įrašų paskyroje), kuriuos pateikia vartotojas, yra suteikiama tik vartotojo pasirinktiems kontaktams. Tačiau galimi atvejai, kai vartotojai gali įgyti daug trečiųjų šalių kontaktų ir kurių iš tikrųjų gali net nepažinoti. Todėl didelis kontaktų skaičius paskyroje, gali būti ženklas, kad vartotojas bus laikomas duomenų valdytoju. Taip pat socialinių tinklų vartotojas gali būti laikomas duomenų valdytoju, kai vartotojo profilio informacija tampa prieinama neapibrėžtam asmenų skaičiui[97].

Pavyzdžiui, internetinės svetainės administratorius, kuris į internetinę svetainę integruoja socialinį modelį ,,Facebook" ,,Patinka" mygtuką, leidžiantį šios svetainės lankytojo naršyklei prašyti minėto modulio teikėjo turinio ir perduoti šiam teikėjui lankytojo asmens duomenis, gali būti laikomas duomenų valdytoju. Vis dėlto tokia atsakomybė jam tenka tik už tą asmens duomenų operaciją arba operacijas, kurių tikslus ir būdus jis realiai nustatė, t. y., už nagrinėjamą duomenų rinkimą ir perdavimą. Vadinasi, jei įmonė integravusi ,,Facebook" mygtuką, pati neturi prieigos prie asmens duomenų, surinktų ir perduotų socialinio modulio teikėjui, su kuriuo kartu jis nustato asmens duomenų tvarkymo būdus ir tikslus, netrukdo tam, kad jis būtų laikomas duomenų valdytoju[98].

Anksčiau galiojo tarytum nerašyta taisyklė, jog gerbėjų tinklalapių (*angl. – fan pages*) administratoriaus atsakomybė, kai pažeidžiamos asmens duomenų apsaugą reglamentuojančios taisyklės, nekyla, ir už tai atsakingas socialinis tinklas. Tačiau ES Teisingumo Teismas savo sprendime nurodė, jog gerbėjų tinklalapio administratorius

[97] ES 29 str. darbo grupės 2019 m. birželio 12 d. Nuomonė Nr. 5/2009 dėl internetinių socialinių tinklų Nr. WP163. [interaktyvus; žiūrėta 2019 m. Spalio 20 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>.

[98] ES Teisingumo Teismo 2019 m. liepos 29 d. sprendimas byloje C-40/17 *Fashion ID & Co. KG*, ECLI:EU:C:2019:629. [Interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: < http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=2333642>.

naudodamasis „Facebook" įdiegta platforma tam, kad galėtų gauti atitinkamas paslaugas, negali būti atleistas nuo pareigų asmens duomenų apsaugos srityje vykdymo. Teismas nurodė, kad gerbėjų tinklalapio sukūrimas „Facebook" apima veiksmus, kuriais administratorius parenka nustatymus, atsižvelgdamas, į jo tikslinę auditoriją ir į veiklos valdymo ir skatinimo tikslus, o šie nustatymai turi įtakos asmens duomenų tvarkymui, siekiant parengti statistinę informaciją remiantis apsilankymais gerbėjų tinklalapyje. Administratorius gali, pasitelkdamas jam „Facebook" suteiktais naudotis filtrais, nustatyti kriterijus, pagal kuriuos ši statistika turi būti rengiama, ir net nurodyti asmenų, kurių asmens duomenis panaudos „Facebook", kategorijas. Todėl „Facebook" esančio gerbėjų tinklalapio administratorius prisideda prie šio tinklalapio lankytojų asmens duomenų tvarkymo. Todėl socialiniame tinkle esančio gerbėjų tinklalapio administratorius, parinkdamas nustatymus, visų pirma, pagal tikslinę auditoriją ir veiklos valdymo ir skatinimo tikslus, dalyvauja gerbėjų tinklalapio lankytojų asmens duomenų tvarkymo ir priemonių nustatymo veikloje. Todėl jis kartu su socialiniu tinklu turi būti laikomas tokių duomenų valdytoju[99].

„Facebook" privatumo nustatymuose yra nurodoma, kad priklausomai nuo aplinkybių, „Facebook" gali būti tiek duomenų valdytojas, tiek duomenų tvarkytojas arba abu vienu metu. Duomenų valdytoju „Facebook" laikomas tuomet, kai jis yra atsakingas už tai, kad nuspręstų, kodėl ir kaip tvarkomi asmens duomenys. Pagal Bendrąjį duomenų apsaugos reglamentą, nustačius, kad „Facebook" laikomas duomenų valdytoju, turėtų paaiškinti kaip duomenys yra renkami, kokie duomenys yra naudojami ir kiek laiko saugomi. Taip pat privalo užtikrinti asmenų prieigą prie šių duomenų. Be to, duomenų valdytojai privalo užtikrinti, kad duomenų tvarkytojai laikytųsi savo sutartinių įsipareigojimų – saugiai ir teisiškai tvarkyti asmenų duomenis. Taip pat yra atvejų, kuomet „Facebook" veikia kaip duomenų tvarkytojas: a) kai socialinis tinklas naudoja įmonės CRM (*liet. - Ryšių su klientais valdymas*) duomenis, kad sukurtų individualią auditoriją reklamos kompanijoms; b) Facebook tvarko duomenis reklamuotojo vardu, kad būtų galima įvertinti reklamos kampanijų našumą ir auditorijos pasiekiamumą bei pranešti apie reklamą pasiekusią auditoriją[100].

Apibendrinant šį skyrių, galima daryti išvadą, jog Bendruoju duomenų apsaugos reglamentu įtvirtintos naujovės duomenų valdytojų atžvilgiu sustiprina jų atsakomybę Reglamentu įtvirtintiems reikalavimams. Bendrajame duomenų apsaugos reglamente

[99] Europos Sąjungos Teisingumo Teismas. 2018 m. birželio 5 d. sprendimas *Wirtschaftsakademie Schleswig-Holstein GmbH* C-210/16, EU:C:2018:388.
[100] Facebook Terms of Service. [žiūrėta internete 2019 m. kovo 15 d.]. Prieiga per internetą: https://www.facebook.com/terms.php.

pareigos formuluojamos abstrakčiai, palikdamos plačią nuožiūros laisvę patiems duomenų valdytojams pasirinkti reguliavimo interpretavimą ir pareigų įgyvendinimo būdus[101]. Be to, socialinių tinklų valdytojais gali būti ne tik socialinių tinklų paslaugų teikėjas, tačiau yra numatyti atvejai, kada duomenų valdytoju tampama ir administruojant socialinio tinklo puslapį, bei esant trečiaja šalimi, naudojant specialias programas, skirtas asmens duomenų rinkimui rinkodaros ar reklamos tikslais.

2.3. Eksteritorialus bendrojo duomenų apsaugos reglamento taikymas

Skaitmeniniame amžiuje jurisdikcija, grindžiama tik teritoriškumo principu, tampa vis mažiau aktuali. Ne taip seniai asmens duomenų tvarkymas atrodė lengvai suprantamas: duomenų valdytojas, duomenų tvarkytojas, duomenų subjektas ir visos priemonės naudojamos duomenų tvarkymo operacijoms įprastai buvo toje pačioje šalyje. Duomenų tvarkymo operacijoms nekildavo jurisdikcijos kolizijų problemų, todėl teritorinio principo taikymas buvo pakankamas užtikrinti asmens duomenų apsaugą. Tokios duomenų tvarkymo procedūros buvo vyraujančios 8-9 dešimtmetyje, kai buvo parengta Europos Tarybos Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu ir ES Direktyva 95/46/EB[102].

Asmens duomenų tvarkymui naudojami metodai, per santykinai trumpą laiką, tapo tarptautinio pobūdžio ir rimtu iššūkiu nacionaliniams įstatymų leidėjams[103]. Technologinė pažanga leido ES gyventojams tvarkyti asmens duomenis už ES ribų anksčiau nematytu mastu[104]. Šiuo metu beveik kiekvienas internete atliekamas veiksmas yra tiesiogiai ar netiesiogiai susijęs su asmens duomenų tvarkymu[105]. Internetas yra globalus tinklas, prieinamas visame pasaulyje, todėl nenuostabu, jog jam turintys įtakos teisės aktai bei teismų sprendimai, gali turėti eksteritorinį taikymą.

Remiantis Bendruoju duomenų apsaugos reglamentu, įtvirtinama eksteritoriali ES duomenų apsaugos taikymo sritis, o duomenų judėjimas į trečiasias šalis leidžiamas tik,

---

[101] ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104, p. 159 – 160.

[102] DE HERT, Paul; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Volume 6, Issue 3, 2016 p. 230–243. [interaktyvus. Žiūrėta 2019 m. kovo 21 d.] Prieiga per internetą: https://academic.oup.com/idpl/article/6/3/230/2447252.

[103] KUNER, Christopher. Extraterritoriality and Regulation of International Data Transfers in EU Data Protection Law 5 International Data Privacy Law 242, 2015.

[104] MOEREL, Lokke. The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? 1 International Data Privacy Law 28, 2011.

[105] KUNER, Christopher. Data Protection Law and International Jurisdiction on the Internet (Part 1)18 International Journal of Law and Information Technology 176, 2010.

jeigu juose teisinio reguliavimo sutartinėmis, korporacinėmis arba kitokiomis priemonėmis, bus užtikrinta ES reguliavimui analogiška duomenų apsauga. Siekdamos naudotis ES esančių asmenų duomenimis, trečiosios šalys, viso pasaulio verslai ir organizacijos ieškos būdų suvienodinti duomenų apsaugos reguliavimą su ES standartais[106].

Bendrojo duomenų apsaugos reglamento 3 straipsnis numato įstatymų leidėjo ketinimą užtikrinti visapusišką ES duomenų subjektų teisių apsaugą ir nustatyti vienodas sąlygas ES rinkose veikiančioms įmonėms, duomenų apsaugos reikalavimų atžvilgiu. Bendrojo duomenų apsaugos reglameno 3 straipsnis apibrėžia reglamento teritorinę taikymo sritį, remdamasis dviem pagrindiniais kriterijais: „įsisteigimo“ kriterijumi, kaip nurodyta 3 straipsnio 1 dalyje, ir „taikymo“ kriterijumi pagal 3 straipsnio 2 dalį. Jei įvykdomas vienas iš šių dviejų kriterijų, atitinkamai duomenų valdytojo arba duomenų tvarkytojo asmens duomenų tvarkymui taikomos Bendrojo duomenų apsaugos reglamento nuostatos[107].

Bendrojo duomenų apsaugos reglamento 3 straipsnio 2 dalis laikoma vienu svarbiausių reformos laimėjimų. Bendrasis duomenų apsaugos reglamentas taikomas ir tokiam duomenų tvarkymui, kai ES esančių duomenų subjektų asmens duomenis tvarko ES neįsisteigęs duomenų valdytojas ar duomenų tvarkytojas, kai duomenų tvarkymo veikla yra susijusi su:

a) prekių arba paslaugų siūlymu tokiems duomenų subjektams Sąjungoje, nepaisant to, ar už šias prekes arba paslaugas duomenų subjektui reikia mokėti;
b) arba elgesio, kai jie veikia ES, stebėsena.

Siekiant nustatyti, ar ES neįsisteigęs duomenų valdytojas ar duomenų tvarkytojas siūlo prekes ar paslaugas ES esantiems duomenų subjektams, turėtų būti įsitikinta, ar akivaizdu, kad tas duomenų valdytojas ar duomenų tvarkytojas ketina teikti paslaugas duomenų subjektams vienoje ar keliose ES valstybėse narėse. Šį ketinimą gali rodyti tam tikri veiksniai: kalbos ar valiutos, įprastai vartojamų vienoje ar keliose valstybėse narėse, vartojimas turint galimybę užsisakyti prekių ir paslaugų kita kalba, arba ES esančių vartotojų ar naudotojų minėjimas. Tai, kad ES yra prieinami duomenų valdytojo, duomenų tvarkytojo ar tarpininko interneto svetainė, elektroninio pašto adresas ar kiti

[106] ZALESKIS, J. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103, p. 45-54. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/10779.
[107] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, 2018. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

kontaktiniai duomenys, savaime neturėtų nulemti ES duomenų apsaugos teisės taikymo[108].

Siekiant nustatyti, ar duomenų tvarkymo veikla gali būti laikoma duomenų subjektų elgesio stebėsena, reikėtų įsitikinti, ar fiziniai asmenys internete 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[109].

Kadangi didžioji dalis socialinių tinklų buveinių yra įsteigtų ne ES, todėl aktualu išanalizuoti, kokiais kriterijais remiantis Bendrasis duomenų apsaugos reglamentas taikomas socialiniams tinklams. Remiantis aukščiau išvardintais dviem kriterijais, galima manyti, jog socialiniai tinklai, kaip duomenų valdytojai ar duomenų tvarkytojai, kurie nėra įsisteigę ES, jų duomenų veikla yra susijusi su elgesio, kai jie veikia ES, stebėsena. Bendrojo duomenų apsaugos reglamento 3 straipnsnio 2 dalies b punktas gali būti taikomas trečiųjų šalių socialinių tinklų operatoriams, interneto paslaugų teikėjams, kurių didžioji dalis sistemingai stebi interneto naudotojų elgesį[110]. Pavyzdžiui, ES Teisingumo Teismas *Google Spain* sprendime paskelbė, kad paieškos sistemų paslaugoms, kurias teikia korporacija, įsikūrusi už Europos sienų, taikomi ES duomenų apsaugos įstatymai[111].

Pagal Bendrojo duomenų apsaugos reglamento 44 bei 45 straipsnius, leidžiama perduoti duomenis į trečiąją valstybę arba tarptautinei organizacijai, jeigu ES Komisija nuspręstų, kad atitinkama trečioji valstybė užtikrina tinkamo lygio apsaugą. Vertindama apsaugos lygio tinkamumą, ES Komisija visų pirma turi atsižvelgti į kelis aspektus – trečiųjų šalių teisinį reguliavimą ir tai, ar jose yra veiksmingai veikianti nepriklausoma duomenų apsaugos priežiūros institucija. Jeigu nebus priimtas ES Komisijos sprendimas dėl tinkamo duomenų apsaugos lygio, duomenų valdytojas arba duomenų tvarkytojas galės perduoti duomenis, jeigu pasirinktų nustatyti bet kurią iš Bendrajame duomenų apsaugos reglamente nurodytų tinkamų duomenų apsaugos priemonių. Kad ir kokią priemonę duomenims perduoti pasirinktų organizacija, visos jos turi užtikrinti, kad

---

[108] 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.

[109] *Ibid.*

[110] DE HERT, Paul; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Volume 6, Issue 3, 2016 p. 230–243. [interaktyvus. Žiūrėta 2019 m. kovo 21 d.] Prieiga per internetą: https://academic.oup.com/idpl/article/6/3/230/2447252.

[111] ES Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas byloje C131/12 *Google Spain and Google*. [Interaktyvus. Žiūrėta 2019 m. spalio 12 d.]. Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN.

nebūtų pakenkta Bendruoju duomenų apsaugos reglamentu garantuojamam fizinių asmenų apsaugos lygiui[112].

2.4. Asmeninių poreikių išimtis

Bendrojo duomenų apsaugos reglamento 2 straipsnio 2 dalies c punkte teigiama, jog Duomenų apsaugos reglamentas netaikomas, kai duomenis tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla. Taip pat, Reglamento preambulės 18 dalyje nurodyta, kad netaikomas tokiais atvejais, kai asmens duomenis fizinis asmuo tvarko vykdydamas grynai asmeninę ar namų ūkio priežiūros veiklą ir nesusiedamas to su profesine ar komercine veikla. Asmeninę ar namų ūkio priežiūros veiklą gali sudaryti, be kita ko, susirašinėjimas ir adresų saugojimas, bei įsigaliojus Bendrajam duomenų apsaugos reglamentui, išimties taikymo sritis buvo praplėsta ir papildyta dviem svarbiais elementais, tai naudojimuosi socialiniais tinklais ir internetine veikla. Tačiau šis reglamentas taikomas duomenų valdytojams arba duomenų tvarkytojams, kurie suteikia priemones asmens duomenų tvarkymui vykdant tokią asmeninę ar namų ūkio priežiūros veiklą[113].

Atsižvelgiant į tai, kad asmenų besinaudojančių internetinėmis paslaugomis skaičius tik auga, vis daugiau asmenų socialiniuose tinkluose naudos informaciją asmeniniais tikslais, todėl egzistuoja poreikis išaiškinti išimties taikymo atvejus. Daugeliu atveju, socialinių tinklų vartotojai laikomi duomenų subjektais. Tačiau, kai kuriais atvejais namų ūkio išimtis negali būti taikoma tam tikrai socialinio tinklo vartotojo veiklai, todėl turi būti laikoma, kad vartotojas prisiėmė kai kurias duomenų valdytojo pareigas. Todėl itin svarbu nustatyti veiklos tikslą bei pobūdį. Socialinių tinklų vartotojų veikla gali peržengti grynai asmeninę ar namų ūkio veiklą, jei vartotojas veikia įmonės ar asociacijos vardu arba naudoja socialinį tinklą daugiausia kaip platformą komerciniams, politiniams ar labdaros tikslams pasiekti, ir tokiu atveju išimtis nebus taikoma. Be to, 29 straipsnio darbo grupės nuomone, vertinant ar duomenų tvarkymas yra atliekamas asmeniniais tikslais, svarbus vertinamasis kriterijus turėtų būti laikomas informacijos teikimas itin plačiam asmenų ratui. Taip pat, kaskart reikėtų apsvarstyti, kad nė vienas asmuo realiame gyvenime neturi neriboto draugų, šeimos narių ar pažįstamų rato, tad asmens duomenų paskelbimas neribotam skaičiui žmonių gali reiškti, kad duomenų

[112] 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.
[113] *Ibid.*

tvarkymas negali būti laikomas asmeniniu ir tokiu atveju nepatektų į išimties taikymo sritį[114]. Taigi grynai asmeninė ar namų ūkio priežiūros veikla, tai yra tik tokia privati veikla, kuri yra asmeninė arba apsiriboja tik savo namų ūkiu ir nesusijusi su jokia profesine ar komercine veikla.

Teismų praktikoje asmeninės ar namų ūkio veiklos sąvoka aiškinama griežtai. Būtinybę taikyti griežtą aiškinimą patvirtina ir pati šios nuostatos formuluotė, pagal kurią iš reguliavimo taikymo srities pašalintas duomenų tvarkymas, atliekamas užsiimant ne paprastai asmenine ar namų ūkio veikla, bet „tik" asmenine ir namų ūkio veikla[115]. Todėl šią išimtį reikia aiškinti kaip numatančią tik tokią veiklą, kuria privatūs asmenys užsiima neperžengdami privataus ar šeimos gyvenimo ribų, o taip akivaizdžiai nėra tvarkant asmens duomenis, kai jie paskelbiami internete ir tampa prieinami neapibrėžtam asmenų skaičiui[116].

Duomenų apsaugos institucijai siekiant nustatyti, ar konkretus duomenų tvarkymas patenka į asmeninio ar namų ūkio tvarkymo sritį, reikia atsižvelgti į šiuos veiksnius:

- ar asmens duomenys yra naudojami neribotam asmenų skaičiui, ar apribotam šeimos, draugų ar pažįstamų ratui;
- ar asmens duomenys yra apie nepažįstamus asmenis;
- jei asmens duomenų tvarkymo mastas bei dažnumas rodo profesinę ar visą darbo dieną vykdomą veiklą;
- jei yra galimas neigiamas poveikis asmenims, įskaitant įsibrovimą į jų privatumą[117].

Visgi išplėtus asmeninės ūkio ar namų priežiūros veiklos sampratą, kuomet asmeninių poreikių išimtis taikoma ir vykdant veiklą socialiniuose tinkluose, nėra iki galo aišku, kokiais kriterijais remiantis nustatyti šios išimties taikymo sritį. Panašu, jog reikalinga nauja ES Teisingumo Teismo praktika, atsižvelgiant į Bendrojo duomenų apsaugos reglamento reguliavimą, kuri išplėstų bei paaiškintų taikymo kriterijus.

Šio darbo autorės nuomone vartotojas socialiniuose tinkluose neturėtų būti pašalintas iš asmeninio naudojimo išimties vien tik remiantis informacijos gavėjų skaičiumi. Išimtis

---

[114] Proposals for Amendments regarding exemption for personal or household activities. Annex 2. The situation under Directive 95/46/EC.

[115] Europos Sąjungos Teisingumo Teismo 2014 m. gruodžio 11 d. sprendimas byloje *Ryneš*, EU:C:2014:2428. [Interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf?docid=160561&doclang=LT.

[116] Europos Sąjungos Teisingumo Teismo 2003 m. lapkričio 6 d. sprendimas byloje *Bodil Lindqvist* C-101/01, EU:C:2003:596. [interaktyvus. Žiūrėta 2019 m. kovo 13 d.]. Prieiga per internetą: http://curia.europa.eu/juris/document/document.jsf?text=&docid=48382&pageIndex=0&doclang=LT&mode=lst&dir=&occ=first&part=1&cid=2550125.

[117] Proposals for Amendments regarding exemption for personal or household activities. Annex 2. The situation under Directive 95/46/EC.

neturėtų būti taikoma tik tuo atveju, jei kišimasis į kitų asmenų privatumo interesus aiškiai viršija įprastos socialinės sąveikos ir interneto naudojimo ribas. Pavydžiui dėl duomenų naudojimo masto ar dažnumo, taip pat duomenų pobūdžio. Kadangi Teisingumo Teismo praktikos šiuo atžvilgiu nėra daug, iškyla daugiau klausimų, nei randama atsakymų.

3.1 PAGRINDINIAI BENDROJO DUOMENŲ APSAUGOS REGLAMENTO REIKALAVIMAI SOCIALINIAMS TINKLAMS

3.1. Asmens duomenų tvarkymo principai

Bendruoju duomenų apsaugos reglamentu siekiama užtikrinti vienodo ir aukšto lygio fizinių asmenų duomenų apsaugą bei nuoseklų ir vienodą taisyklių, kuriomis reglamentuojama fizinių asmenų pagrindinių teisių ir laisvių apsauga tvarkant asmens duomenis, taikymą[118]. Šiam tikslui pasiekti Bendrojo duomenų apsaugos reglamento 5 straipsnis įtvirtina šešis principus, kuriais savo veikloje yra įpareigoti vadovautis visi duomenų tvarkytojai ir duomenų valdytojai tam, kad bet koks asmens duomenų tvarkymas atitiktų šio reglamento reikalavimus ir būtų užtikrinta duomenų subjekto teisių apsauga. Su asmens duomenų tvarkymu susiję principai teisine prasme nėra absoliuti naujovė. Reglamentas ne tik įtvirtina naujus atskaitomybės bei skaidrumo principus, bet ir papildomai sureguliuoja iki šiol galiojusius, praplėsdamas jų turinį[119].

Taigi, asmens duomenys duomenų subjekto atžvilgiu turi būti tvarkomi teisėtu, sąžiningu ir skaidriu būdu[120]. Duomenų tvarkymo teisėtumo, sąžiningumo ir skaidrumo principas – svarbiausias, plačiausios apimties ir abstrakčiausias duomenų apsaugos teisės principas. Teisėtumą, sąžiningumą ir skaidrumą galima laikyti atskirais duomenų apsaugos teisės principais. Iš esmės visas duomenų apsaugos teisės reguliavimas detalizuoja šį principą, įtvirtindamas konkrečius teisėto, sąžiningo ir skaidraus duomenų tvarkymo aspektus[121].

Reglamentas aiškiai nurodo, kad duomenų tvarkymas būtų teisėtas, asmens duomenys turi būti tvarkomi gavus atitinkamo duomenų subjekto sutikimą. Sutikimas turėtų būti duodamas aiškiu aktu patvirtinant, kad yra suteiktas laisva valia, konkretus, informacija pagrįstas ir vienareikšmis nurodymas (pavyzdžiui, raštiškas, įskaitant elektroninėmis priemonėmis, arba žodinis pareiškimas, kuriame duomenų subjektas

[118] 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, preambulė 10 d.
[119] ŠTAREIKĖ, E. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, S. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018, p. 293 – 312.
[120] 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.
[121] BYGARVE, Lee Andrew. Data protection Law. Approaching Its Rationale, Logic and Limits. Dordrech: Kluwer Law International, 2002, p. 58-59.

sutinka su juo susijusių asmens duomenų tvarkmu[122]. Remiantis atskaitomybės principu duomenų valdytojui tenka atsakomybė įrodyti, kad duomenų subjektas sutiko su duomenų tvarkymu bei pateiktas sutikimas atitinka Reglamente nustatytus turinio reikalavimus.

Sąžiningumo principas reiškia bendrojo pobūdžio duomenų valdytojų ir duomenų tvarkytojų pareigą sąžiningai tvarkyti duomenis. Nei duomenų apsaugos teisėje, nei kitose teisės srityse sąžiningumo principo turinys nėra išsamiai ir oficialiai apibrėžtas. Tai, ar duomenys tvarkomi sąžiningai, turi būti vertinama kiekvienu konkrečiu atveju, atsižvelgiant į faktines aplinkybes[123].

Skaidrumas paprastai laikomas vienu iš viešojo sektoriaus subjektų veiklos standartų. Duomenų tvarkymo skaidrumas yra neatsiejamas nuo sąžiningumo ir atskaitomybės principų. Konstitucinis Teismas yra konstatavęs, kad skaidrumas suponuoja informacijos sklaidą ir komunikavimą, atvirtumą ir viešumą (tiek, kiek tai nekenkia kitoms teisės saugomoms vertybėms), atskaitingumą atitinkamai bendruomenei. Pasak Konstitucinio Teismo, skaidrumas sąlygoja ir reikalavimą, kad priimami sprendimai būtų pagrįsti, aiškūs, kad, iškilus reikalui, jie būtų racionaliai motyvuoti, o asmenys turėtų galimybę priimtus sprendimus ginčyti nustatyta tvarka[124]. Šiame kontekste svarbu paminėti ES Teisingumo Teismo praktiką, kurioje teismas yra nurodęs, kad skaidrumo principas leidžia piliečiams artimiau dalyvauti sprendimų priėmimo procese, garantuoja didesnį valdymo teisėtumą ir veiksmingumą, aukštesnį atskaitomybės piliečiams mastą demokratinėje sistemoje[125].

Taikant skaidrumo principą, fiziniams asmenims turėtų būti aišku, kaip su jais susiję asmens duomenys yra renkami, naudojami, kaip su jais susipažįstama arba kaip jie yra tvarkomi, taip pat kokiu mastu asmens duomenys yra ar bus tvarkomi. Pagal

---

[122] *Ibid.*

[123] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija, VĮ Registrų centras, 2019, p. 114.

[124] Lietuvos Respublikos Konstitucinio Teismo 2008 m. sausio 22 d. nutarimas „Dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Priėmimo į valstybės tarnautojo pareigas tvarkos patvirtinimo“ (2002 m. birţelio 24 d., 2002 m. rugpjūčio 29 d., 2003 m. birţelio 3 d., 2003 m. lapkričio 25 d., 2005 m. spalio 28 d. redakcijos) patvirtintos Priėmimo į valstybės tarnautojo pareigas tvarkos atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos įstatymo 3 straipsnio (2002 m. balandţio 23 d. redakcija) 1 daliai, dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2006 m. birţelio 28 d. redakcija) patvirtinto Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos įstatymo 3 straipsnio (2002 m. balandţio 23 d., 2007 m. birţelio 7 d. redakcijos) 1 daliai, taip pat dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2007 m. rugsėjo 26 d., 2007 m. gruodţio 12 d. redakcijos) patvirtinto Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos įstatymo 3 straipsnio (2007 m. birţelio 7 d. redakcija) 1 daliai“. Valstybės ţinios. 2008, Nr. 10-350.

[125] Europos Sąjungos Teisingumo Teismas. 2003 m. kovo 6 d. sprendimas *Interporc Im, Export GmbH v. Komisija* C-41/00, EU:C:2003:125.

skaidrumo principą informacija ir pranešimai, susiję su asmens duomenų tvarkymu, turi būti lengvai prieinami ir suprantami, pateikiami aiškia ir paprasta kalba. Skaidrumo principas, visų pirma, susijęs su duomenų subjektų informavimu apie duomenų valdytojo tapatybę ir duomenų tvarkymo tikslus, taip pat su tolesniu informavimu, kad būtų užtikrintas sąžiningas ir skaidrus duomenų tvarkymas atitinkamų fizinių asmenų atžvilgiu, jų teisė gauti patvirtinimą, dėl su jais susijusių asmens duomenų tvarkymo ir teisė tuos duomenis gauti. Fiziniai asmenys turėtų būti informuoti apie su asmens duomenų tvarkymu susijusius pavojus, taisykles, apsaugos priemones bei teises ir apie tai, kaip naudotis savo teisėmis tokio asmens duomenų tvarkymo srityje[126].

Bendrajame duomenų apsaugos reglamente įtvirtintas reikalavimas, pagal kurį sąžiningo ir skaidraus duomenų tvarkymo principus duomenų subjektui pranešama apie vykdomą duomenų tvarkymo operaciją ir jos tikslus. Duomenų valdytojas turėtų pateikti duomenų subjektui visą papildomą informaciją, kuri būtina tam, kad būtų užtikrintas sąžiningas ir skaidrus duomenų tvarkymas, atsižvelgiant į konkrečias asmens duomenų tvarkymo aplinkybes ir kontekstą[127]. ES 29 straipsnio darbo grupė nurodo, kad skaidrumo principas yra taikomas trims pagrindinėms sritims: a) informacijos, susijusios su sąžiningu duomenų tvarkymu, teikimu duomenų subjektui; b) duomenų valdytojo bendravimui su duomenų subjektais dėl jų teisių pagal Bendrąjį duomenų apsaugos reglamentą; c) duomenų valdytojo teisių įgyvendinimo palengvinimui duomenų subjektui[128]. Be to, ES 29 straipsnio darbo grupės nuomone, skaidrumo principo koncepcija yra orientuota į duomenų subjektą.

Socialinis tinklas „Facebook" privatumo politikoje nurodo, kad skaidrumo principą siekiama įgyvendinti, duomenų politiką paliekant vienintele konsoliduota vieta, kurioje aprašomi būdai kaip socialinis tinklas naudoja duomenis ir kaip juos tvarko, taip pat jie ruošiasi suteikti asmenų švietimą per sutikimo galimybę naujiems ir esamiems vartotojams[129]. Socialiniam tinklui atnaujinus privatumo politiką, galima daryti išvadą, jog informacija tapo prieinamesnė, tačiau vartojama kalba, bei paini nuorodų taikymo praktika lieka virs dar neaiški paprastam vartotojui. Galima sakyti, jog socialinis tinklas „Facebook" skaidrumo principą išpildo formaliai informuodamas vartotojus, kaip su jais

[126] 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.
[127] *Ibid.*
[128] ES 29 str. darbo grupė. *Guidelines on transparency under Regulation 2016/679, Nr. WP 260, p. 4.* [interaktyvus, 2019 m. balandžio 5 d.]. Prieiga per internetą: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.
[129] Facebook privatumo politika. [interaktyvus, Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: https://www.facebook.com/policy.php

susiję asmens duomenys yra renkami ir naudojami, pasiūlyta platforma susipažinti su kaupiamais duomenimis, bei paaiškinama, kaip jie yra tvarkomi. Tačiau neaiškumų kyla ties galimybe sužinoti, kokios apimties asmens duomenys yra ir bus tvarkomi[130].

Duomenų apsaugos reglamentas įpareigoja duomenų valdytojus prisiimti kuo daugiau atsakomybės už asmens duomenų tvarkymą, tokiu būdu netiesiogiai išreiškiant pasitikėjimą valdytojų atliekamais veiksmais, bet kartu sugriežtinant valdytojų pareigas duomenų apsaugos srityje. Šiame kontekste itin reikmingas atskaitomybės principas, kuris įpareigoja duomenų tvarkytoją ar duomenų valdytoją būti atsakingais už duomenų apsaugos reikalavimų laikymąsi[131]. 29 straipsnio darbo grupės nuomone, šis principas skirtas užtikrinti, kad duomenų valdytojai būtų labiau kontroliuojami ir galėtų praktiškai užtikrinti, ir įrodyti duomenų apsaugos principų laikymąsi. Be to, atskaitomybė reikalauja, kad duomenų valdytojai įdiegtų vidaus mechanizmus ir kontrolės sistemas, užtikrinančias atitiktį ir pateiktų įrodymus[132]. Negana to, duomenų valdytojas ar duomenų tvarkytojas turi sugebėti įrodyti, jog duomenys tvarkomi laikantis Reglamento reikalavimų.

Bendriausia prasme, atskaitomybės principas apima du didelės apimties elementus. Pirma, reikalaujama organizacijose taikyti tinkamą vidaus politiką ir priemones, skirtas užtikrinti, kad būtų laikomasi esminių duomenų apsaugos teisės principų ir prievolių. Antra, atskaitomybės principas reiškia, kad duomenų valdytojai turi turėti vidinius mechanizmus, kad galėtų įrodyti Bendrojo duomenų apsaugos reglamento atitiktį suinteresuotiems asmenims, visų pirma – priežiūros institucijoms[133].

Taigi, socialinis tinklas, veikdamas kaip duomenų valdytojas, įgyvendindamas Bendrojo duomenų apsaugos reglamento 5 straipsnio 2 dalyje įtvirtintą atskaitomybės principą, yra atsakingas už tai, kad būtų sukurta tinkama duomenų politika ir, kad būtų laikomasi su asmens, šiuo atveju socialinio tinklo vartotojo, duomenų tvarkymu susijusių principų, ir turi sugebėti įrodyti, kad jų laikomasi. Šiuo atveju, socialiniai tinklai privatumo politikose privalo nurodyti, kokiais atvejais socialinis tinklas yra duomenų valdytojas, o kuriais duomenų tvarkytojas.

---

[130] Facebook privatumo politika. [interaktyvus, Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: https://www.facebook.com/policy.php

[131] ŠTAREIKĖ, Eglė. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, S. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018, p. 293 – 312.

[132] Article 29 Data Protection Working Party. *Opinion 3/2010 on the principle of accountability.* 00062/10/EN WP 173, p, 3.

[133] ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. Monografija, VĮ Registrų centras, 2019, p. 135.

Duomenų kiekio mažinimo principas tiesiogiai siejamas su asmens duomenų saugojimo laikotarpiu. Bendrasis duomenų apsaugos reglamentas išlieka nuoseklus ir duomenų valdytojus įpareigoja užtikrinti, kad duomenų saugojimo laikotarpis būtų minimalus ir pagrįstas bei nustatomas įvertinus poreikį juos tvarkyti, atsižvelgiant į duomenų tvarkymo tikslus. Pažymėtina, jog Bendrasis duomenų apsaugos reglamentas nenustato minimalaus ar maksimalaus duomenų saugojimo laikotarpio, todėl kiekviena įstaiga privalo individualiai nusistatyti terminus, per kiek laiko saugomi duomenys, turi būti ištrinti[134]. Be to, duomenų kiekio mažinimo principo požiūriu gali būti tvarkomi tokie asmens duomenys ir tokiu būdu, kad būtų daromas mažiausias neigamas poveikis duomenų subjekto interesams[135]. Taip pat leidžiama tvarkyti tik tuos asmens duomenis, kurie neišvengiamai reikalingi asmens duomenų tvarkymo tikslams pasiekti. Ketinamų tvarkyti asmens duomenų kategorijos privalo būti duomenų valdytojo identifikuotos prieš pradedant rinkti asmens duomenis. Taip pat, asmens duomenys, kurie nėra būtini asmens duomenų tvarkymo tikslams pasiekti, laikomi pertekliniais šių tikslų požiūriu, o jų rinkimas, kaupimas, kitoks tvarkymas – pažeidžiančiais duomenų subjekto ir duomenų valdytojo interesų pusiausvyrą[136]. Apžvelgiant į socialinio tinklo ,,Facebook" privatumo politiką nėra aiškiai nurodoma, kiek laiko asmens duomenys yra ar bus saugomi socialiniame tinkle, kai vartotojai naudojasi socialiniu tinklu. Pateikiama informacija, tik apie duomenų kaupimo laikotarpį, kai vartotojas išsiregistruoja. Nurodoma, kad vartotojas negalės rasti ištrintos informacijos ar turinio, kadangi ištrintos paskyros turinys taip pat yra ištrinamas iš ,,Facebook" serverių.

Tikslo apribojimo principas tiesiogiai suponuoja duomenų kiekio mažinimo principą, kuris laikomas besąlygiška asmens duomenų apsaugos dalimi ir visuotinai pripažįstamas, kaip vienas iš geros praktikos aspektų. Šio principo esmė yra tokia, kad duomenų valdytojas ne tik neturėtų rinkti asmens duomenų be jokių aiškių ir apibrėžtų tikslų, bet ir tai, kad turi būti renkami tik tokie duomenys, kurie yra adekvatūs bei susiję su tais tikslais, kuriais jie tvarkomi ir ribojami pagal tai, kiek jų yra būtina turėti atsižvelgiant į tikslus, kuriais jie tvarkomi[137]. Socialiniai tinklai, tokie kaip ,,Facebook" ar

[134] ES duomenų apsaugos taisyklių reforma. [interaktyvus. Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-long-can-data-be-kept-and-it-necessary-update-it_lt.

[135] Europos Ţmogaus Teisių Teismas. Teismas 2008 m. gruodžio 4 d. sprendimas *S. ir Marper prieš Jungtinę Karalystę*, Nr. 30562/04, 30566/04, §78-86.

[136] KERR, Ian, STEEVES, Valerie, LUCOCK, Carole. Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society. Oxford: Oxford University Press, 2009. p. 35

[137] ŠTAREIKĖ, Eglė. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, Sigita. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018, p. 293 – 312.

„Twitter", privatumo politikose tikslo apribojimo principą pritaikė, išsamiai nurodydami, kokie asmens duomenys ir kokiais konkrečiais tikslais yra renkami[138].

Reglamento 5 straipsnio 1 dalies d punkte įtvirtintas duomenų tikslumo principas įpareigoja duomenų valdytoją imtis visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi [139]. Kadangi asmens duomenų tikslumas ir išsamumas vertinami, atsižvelgiant į asmens duomenų tvarkymo tikslus, kurie vadovaujantis minimalaus būtino asmens duomenų tvarkymo principu ir kitais asmens duomenų teisinės apsaugos srityje veikiančiais principais, turi būti nustatyti prieš pradedant rinkti asmens duomenis ir turi atitikti realius duomenų valdytojo pereikius [140]. Svarbi prielaida tvarkomų asmens duomenų tikslumui užtikrinti, tai rūpestingas šaltinių, iš kurių bus renkami asmens duomenys, parinkimas. Taip pat svarbu užtikrinti, kad asmens duomenys būtų atnaujinami laiku, o pasenę duomenys nebūtų naudojami. Duomenų subjektas turėtų turėti teisę reikalauti, kad jo asmens duomenys būtų ištrinti ir toliau nebetvarkomi, kai asmens duomenų nebereikia tiems tikslams, kuriais jie buvo renkami ar kitaip tvarkomi, kai duomenų subjektas atšaukė savo sutikimą ar nesutinka, kad jo asmens duomenys būtų tvarkomi.

Konfidencialumo principas taip pat nėra naujovė duomenų apsaugos kontekste, tačiau Bendrajojo duomenų apsaugos reglamento 5 straipsnio 1 dalies f punkte jis įtvirtintas kartu su vientisumo principu. Duomenų valdytojas ar duomenų tvarkytojas privalo taikyti atitinkamas technines ar organizacines priemones užtikrinti tinkamą asmens duomenų saugumą, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo.

Siekiant užtikrinti saugumą ir užkirsti kelią netinkamam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones, pavyzdžiui, šifravimą. Šiomis priemonėmis turėtų būti užtikrintas tinkamo lygio saugumas, įskaitant konfidencialumą, atsižvelgiant į techninių galimybių išsivystymo lygį ir įgyvendinimo sąnaudas, pavojų ir saugotinų asmens duomenų pobūdžio atžvilgiu. Vertinant pavojų duomenų saugumui, reikėtų atsižvelgti į pavojus, kurie kyla tvarkant asmens duomenis, pavyzdžiui, į tai, kad

[138] Facebook privatumo politika. [interaktyvus, Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: https://www.facebook.com/policy.php>.; Twitter privatumo politika. [interaktyvus. Žiūrėta 2019 m. spalio 10 d.]. Prieiga per internetą: <https://twitter.com/en/privacy>.

[139] 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.

[140] PETRAITYTĖ, Ilona. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.

persiųsti, saugomi ar kitaip tvarkomi duomenys gali būti netyčia arba neteisėtai sunaikinti, prarasti, pakeisti, be leidimo atskleisti arba be leidimo prie jų gauta prieiga, ir dėl to visų pirma gali būti padarytas kūno sužalojimas, materialinė ar nematerialinė žala[141]. Be to, kaip vieną iš techninių ar organizacinių priemonių Reglamentas nurodo pseudonimų suteikimą, t.y. procesas, kai asmens duomenys tvarkomi taip, jog jų nebūtų galima susieti su konkrečiu asmeniu, nepasinaudojus papildoma informacija, o ta papildoma informacija yra saugoma atskirai nuo asmens duomenų[142].

3.2. Duomenų tvarkymo pagrindai

Siekiant išvengti situacijų, kai asmens duomenys yra tvarkomi neteisėtai, visuomet būtina atsižvelgti į bendruosius duomenų apsaugos principus. ES Pagrindinių teisių chartijos 8 straipsnio 2 dalyje nurodyta, kad asmens duomenys turi būti tvarkomi atitinkamo asmens sutikimu arba kitu teisėtu, įstatymu nustatytu pagrindu[143]. Teisėtumo principas numatytas Bendrajame duomenų apsaugos reglamente, kuriame reikalaujama, kad asmens duomenys, duomenų subjekto atžvilgiu, būtų tvarkomi teisėtai, sąžiningai ir skaidriai. Duomenų tvarkymas yra teisėtas, jeigu asmens duomenys tvarkomi gavus atitinkamo duomenų subjekto sutikimą arba remiantis kitu teisėtu teisiniu pagrindu[144].

Remiantis Bendrojo duomenų apsaugos reglamento 6 straipsniu, duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu taikoma bent viena iš šių sąlygų:

- Sutikimas. Privalo būti gautas duomenų subjekto sutikimas, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais;
- Sutarties sudarymas. Tvarkyti duomenis būtina, siekiant įgyvendinti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį;
- Teisinis įpareigojimas. Duomenų tvarkymas yra būtinas teisinei prievolei įvykdyti;
- Gyvybiniai interesai. Tvarkyti duomenis yra būtina, siekiant apsaugoti gyvybiškai svarbius duomenų subjekto ar kito fizinio asmens interesus;

---

141 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.

142 ŠTAREIKĖ, Eglė. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, Sigita. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018, p. 293 – 312.

143 Europos Sąjungos pagrindinių teisių chartija. OL C 326, 2012 10 26, p. 391-407.

144 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.

- Užduotis susijusi su visuomenės interesu. Tvarkyti duomenis būtina, siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas;
- Teisėti interesai. 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, ypač kai duomenų subjektas yra vaikas[145].

Asmens duomenų tvarkymas turi būti grindžiamas bent viena iš šių sąlygų. Taip pat svarbu paminėti, kad tarp teisėtų duomenų tvarkymo sąlygų nėra hierarchijos. Tačiau, 29 straipsnio darbo grupė išaiškino, kad duomenų valdytojas, tvarkantis specialias duomenų kategorijas, negali remtis tik bendrais duomenų tvarkymo pagrindais, būtina remtis ir duomenų apsaugos principais[146].

Analizuojant tvarkymo teisėtumą socialinių tinklų kontekste, būtina peržvelgti populiariausio socialinio tinklo privatumo politiką. Socialinio tinklo „Facebook" duomenų politikoje vis dėlto lieka neaišku, kokį tikslų duomenų tvarkymo pagrindą socialinis tinklas pasirinko. Duomenų valdytojas savo privatumo politikoje tiesiog išvardina visus šešis teisėto tvarkymo pagrindus pagal Bendrojo duomenų apsaugos reglamento 6 straipsnį, tiksliai nenurodydamas, kokiu teisiniu pagrindu duomenų valdytojas remiasi, kiekvienoje konkrečioje duomenų tvarkymo operacijoje. Todėl neįmanoma nustatyti, kurios tikslios duomenų tvarkymo operacijos grindžiamos kiekvienu konkrečiu teisiniu pagrindu pagal Bendrojo duomenų apsaugos reglamento 6 ir 9 straipsnius[147]. Tokiu atveju galima manyti, jog socialinis tinklas, įsigaliojus Bendrajam duomenų apsaugos reglamentui, nusprendė formaliai pritaikyti Reglamento reikalavimus. Duomenų politikoje pateikiamos nuorodos į kitus puslapius, kuriuose siūloma sužinoti daugiau apie teisinius tvarkymo pagrindus ir kaip jie susiję su duomenų tvarkymo būdais. Būtent ten išskiriamos tam tikros kategorijos, kurių pagrindu yra taikomos sutarties sąlygos, tai: siekiant suasmeninti, patobulinti Facbook produktus, skatinant saugumą, vientisumą siūlomų paslaugų, ar renkant, saugant bei tvarkant duomenis už ES ribų, įskaitant JAV ar kitas šalis. Facebook taip pat nurodo,

[145] 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.

[146] ES 29 str. darbo grupės 2014 m. balandžio 9 d. Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį Nr. WP217. [interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf>.

[147] 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.

kad galioja kiti teisiniai pagrindai, kuriais remiasi tam tikrais atvejais tvarkydamas vartotojo duomenis. Vienas jų - vartotojo duotas sutikimas. Nuo tada, kai Bendrasis duomenų apsaugos reglamentas įsigaliojo, privatumo politikoje nurodoma, kad „Facebook" savo tvarkymo teisėtumą pagrindžia vartotojo sutikimu su paslaugų teikimo sąlygomis, paspaudžiant mygtuką „Registruotis"[148]. Privatumo politikoje nurodoma, kad socialiniam tinklui „Facebook", kaip duomenų valdytojui, reikalingas vartotojo sutikimas, kai tvarkomi duomenys su specialiomis apsaugomis (pavyzdžiui, religinės pažiūros, politinės pažiūros, sveikatos duomenys), naudojant veido atpažinimo technologiją, norint naudoti duomenis, kuriuos reklamuotojai bei kiti partneriai teikia „Facebook" informaciją apie vartotojo veiklą, dalijantis duomenimis, kurie vartotoją identifikuoja bei norint rinkti informaciją, kurią vartotojas leidžia gauti, naudojantis įgalintais įrenginio nustatymais (pavyzdžiui, prieiga prie GPS vietos, fotoaparato arba nuotraukų)[149]. Tačiau visais atvejais socialinis tinklas „Facebook" reikalauja, kad duomenų subjektas (vartotojas) sutiktų su visa privatumo politika. Todėl galima manyti, jog visas duomenų tvarkymas socialiniame tinkle grindžiamas sutikimu[150].

Svarbu paminėti, kad duomenų subjekto sutikimu laikomas 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[151]. Tuomet iškyla problema, ar sutikimas su privatumo politika, su kuriomis vartotojai privalo sutikti, kad galėtų naudotis socialinių tinklų paslaugomis, yra savanoriškas sutikimas pagal Bendrojo duomenų apsaugos reglamento 6 straipsnio 1a dalį. Pagal Bendrojo duomenų apsaugos reglamento įtvirtintą bendrą taisyklę, jei duomenų subjektas neturi realaus pasirinkimo, jaučiasi priverstas sutikti arba patirtų neigiamų pasekmių, jei sutikimo neduotų, toks sutikimas negalioja[152].

Daugeliui vartotojų, vienintelis pasirinkimas yra sutikti su socialinio tinklo sąlygomis arba nesinaudoti teikiamomis paslaugomis. Kitaip tariant, jeigu vartotojas nesutinka su socialinio tinklo Facebook privatumo politika, jis negali naudotis socialinio

---

[148] Facebook data policy. [interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: https://www.facebook.com/about/privacy/update.

[149] *Ibid.*

[150] Complaint Under Article 77(1) DGPR. [interaktyvus. Žiūrėta 2019 m. lapkričio 22 d.]. Prieiga per internetą: <https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf>.

[151] 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.

[152] 29 str. Darbo grupės 2011 m. liepos 13 d. Nuomonė dėl sąvokos „sutikimas" apibrėžties Nr. WP187. [interaktyvus; žiūrėta 2019 m. spalio 21 d.]. Prieiga per internetą: <https://www.pdpjournals.com/docs/88081.pdf>.

tinklo paslaugomis bei turėti prieigos prie turinio[153]. Todėl, jei sutikimas yra neatskiriamai sujungtas su sąlygomis kaip jų dalis, dėl kurios nesiderama, jis laikomas ne laisva valia duotu sutikimu. Taigi, sutikimas nebus laikomas laisvu sutikimu, jei duomenų subjektas negalės atsisakyti sutikti arba duoto sutikimo atšaukti, nepatirdamas žalos[154].

Siekiant apibrėžti sutikimo nedviprasmiškumą, reikia naudoti mechanizmus, nepaliekančius jokių abejonių dėl duomenų subjekto ketinimo sutikti. Būtent savanoriškumo požiūriu turėtų būti įvertinta, ar asmuo turi tikrą pasirinkimą sutikti dėl savo duomenų tvarkymo. Be to, sutikimas neturėtų būti laikomas duotas laisva valia, jei duomenų subjektas faktiškai neturėjo galimybės laisvai rinktis ar negalėjo atsisakyti sutikti arba atšaukti sutikimo nepatirdamas žalos[155]. Pagal Bendrojo duomenų apsaugos reglamento 7 straipsnio 4 dalį, sprendžiant ar sutikimas duotas laisva valia, daugiausia atsižvelgiama į tai, ar, *inter alia*, yra nustatyta sutarties vykdymo sąlyga (įskaitant paslaugos teikimą), kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti[156].

Laikoma, kad sutikimas nebuvo duotas laisva valia, jeigu neleidžiama duoti atskiro sutikimo atskiroms asmens duomenų tvarkymo operacijoms, nors tai ir tikslinga atskirais atvejais, arba jeigu sutarties vykdymas, įskaitant paslaugos teikimą, priklauso nuo sutikimo, neatsižvelgiant į tai, kad toks sutikimas nėra būtinas tokiam vykdymui[157].

3.3. Duomenų apsaugos pareigūno funkcija

Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalyje įtvirtinta ne teisė, o pareiga tam tikrai daliai duomenų valdytojų ir tvarkytojų paskirti duomenų apsaugos pareigūną. Duomenų apsaugos pareigūnas – tai darbuotojas ar išorės ekspertas (paslaugos teikėjas), kuris prižiūri duomenų valdytojo ar duomenų tvarkytojo atitiktį Bendrajam

[153] MALINAUSKAITĖ-VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017, p 83.
[154] 29 str. Darbo grupės 2011 m. liepos 13 d. Nuomonė dėl sąvokos „sutikimas" apibrėžties Nr. WP187. [interaktyvus; žiūrėta 2019 m. spalio 21 d.]. Prieiga per internetą: <https://www.pdpjournals.com/docs/88081.pdf>.
[155] 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.
[156] *Ibid.*
[157] *Ibid.*

duomenų apsaugos reglamentui ir padeda jį užtikrinti[158]. Pagal Reglamento 37 straipsnio 5 dalį, duomenų apsaugos pareigūnas privalo pasižymėti profesinėmis savybėmis, visų pirma, duomenų apsaugos teisės ir praktikos ekspertinėmis žiniomis[159]. 29 straipsnio darbo grupės teigimu, duomenų apsaugos pareigūnas pripažįstamas vienu pagrindinių dalyvių naujoje duomenų valdymo sistemoje, o Reglamentu nustatomos jo paskyrimo sąlygos, statusas ir užduotys[160]. Duomenų apsaugos pareigūno paskyrimas nulemia Bendrojo duomenų apsaugos reglamento įgyvendinimo procesą, poreikį peržiūrėti organizacinę struktūrą, žmogiškuosius ir finansinius išteklius. Anksčiau galiojusi Direktyva 95/46/EB nenumatė pareigos paskirti duomenų apsaugos pareigūną. Tačiau kaip jau buvo minėta anksčiau, Bendruoju duomenų apaugos reglamentu įtvirtinta naujovė, skatina pasitikėjimą duomenų valdytojais, įpareigodama juos prisiimti daugiau atsakomybės už duomenų tvarkymą ir mažina priežiūros institucijos kišimąsi į kasdienę duomenų tvarkymo veiklą[161]. Be to, duomenų apsaugos pareigūnas neturi gauti nurodymų dėl užduočių įvykdymo, taip pat jo negalima atleisti ar bausti, dėl jam nustatytų užduočių atlikimo. Duomenų apsaugos pareigūnas, kaip nurodyta Bendrajame duomenų apsaugos reglamente, tiesiogiai atsiskaito duomenų valdytojo ar duomenų tvarkytojo aukščiausio lygio vadovybei[162]. Remiantis Bendrojo duomenų apsaugos reglamento 37 straipsnio 1 dalimi, yra numatyti trys atvejai, kuomet duomenų apsaugos pareigūno paskyrimas yra privalomas:

1) kai duomenų tvarkymą atlieka valdžios institucija ar įstaiga, išskyrus teismą, kai jis vykdo teismo funkcijas;
2) arba kai duomenų valdytojai arba duomenų tvarkytojai, kurių pagrindinė veikla yra duomenų tvarkymo operacijos, kurios dėl savo pobūdžio, aprėpties ir (arba) tikslų reikalauja reguliariai ir sistemingai dideliu mastu stebėti duomenų subjektus;

---

[158] ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017, t. 104, p. 159 – 160.

[159] 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.

[160] ES 29 str. darbo grupė. *2016 m. gruodžio 13 d. Gairės dėl duomenų apsaugos pareigūnų (DAP), Nr. WP 243*. [interaktyvus. Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>.

[161] ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103, p. 45-54. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/view/10779.

[162] 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.

3) arba kai duomenų valdytojai arba duomenų tvarkytojai, kurių pagrindinė veikla yra specialiųjų kategorijų duomenų, duomenų apie apkaltinamuosius nuosprendžius ir nusikalstamas veikas tvarkymas dideliu mastu[163].

Reglamento 37 straipsnio 4 dalyje numatyta, jog yra kitų atvejų, kuomet pareigūno skyrimas galimas ir kitais nenurodytais atvejais. Pagal anksčiau minėtus kriterijus, darytina išvada, jog pareigūno skyrimas privalomas organizacijoms, kurios dėl savo veiklos bei jos dydžio ir tikslų kelia didesnę riziką asmens duomenims.

Pirmiausia, neaiškumų kyla dėl ,,pagrindinės veiklos" sąvokos. Ji susijusi su pagrindiniais organizacijos uždaviniais, tokiais kaip, pagrindinėmis operacijomis, reikalingoms organizacijos tikslams pasiekti. Pagrindinė veikla neapima pagalbinės veiklos[164].

Antra, sąvokos ,,reguliariai" ir ,,sistemingai", kurias plačiau aptarė 29 str. darbo grupė, nurodoma, jog sąvoka ,,sisteminga" suprantama, kaip vykstanti pagal sistemą arba iš anksto nustatyta, organizuota ar metodinė, arba vykstanti kaip bendro duomenų rinkimo plano dalis ar strategijos dalis. O ,,reguliari" gali būti apibrėžiama kaip vykstantis arba pasitaikantis, tam tikrais intervalais, konkrečiu laikotarpiu, pasikartojantis konkrečiu metu arba vykstantis nuolat, arba periodiškai. Reguliaria ir sisteminga duomenų subjektų stebėsena gali būti laikoma tokia veikla: asmenų profiliavimas rizikos vertinimo tikslais, asmens buvimo vietos stebėjimas mobiliųjų telefonų programėlėmis, lojalumo programų vykdymas ir kiti[165].

Atsižvelgiant į numatytus reikalavimus, panašu, jog socialiniai tinklai turėtų paskirti duomenų apsaugos pareigūną. Kaip numatyta 37 str. 1 dalies 2 punkte, duomenų pareigūnas skiriamas, jei duomenų valdytojas, kurio pagrindinė veikla yra duomenų tvarkymo operacijos, dėl kurių pobūdžio, aprėpties ir (arba) tikslų būtina reguliariai ir sistemingai, dideliu mastu stebėti duomenų subjektus. Taigi, kaip buvo aptarta ankstesniuose skyriuose, socialinio tinklo viena pagrindinių veiklų yra susijusi su duomenų tvarkymu. Taip pat didžiulė socialinių tinklų vartotojų gausa nulemia socialinio tinklo poreikį reguliariai ir sistemingai stebėti duomenų subjektus. Todėl darytina išvada, kad socialinis tinklas, kaip duomenų valdytojas, atitinka reikalavimą, pagal kurį privaloma skirti duomenų apsaugos pareigūną.

---

[163] 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.
[164] ES 29 str. Duomenų apsaugos darbo grupė. 2016 m. gruodžio 13 d. Duomenų apsaugos pareigūnų gairės (su paskutiniais pakeitimais 2017 m. balandžio 5 d.), Nr. 16/LT WP 243 rev. 01, p. 9-10.
[165] *Ibid*. p., 9-10.

Kad duomenų apsaugos pareigūnas žinotų, kaip tvarkyti asmens duomenis socialiniuose tinkluose, jam labai svarbu: a) suprasti galimas socialinių tinklų sukeliamas pasekmes duomenų subjektų teisėms ir laisvėms. Pagal Bendrojo duomenų apsaugos reglamento 6 straipsnį, teisėti duomenų valdytojo interesai gali būti teisėtas duomenų tvarkymo pagrindas, išskyrus atvejus, kai minėti interesai yra už juos viršesni, ypač kai duomenų subjektas yra vaikas[166]. Taip pat, duomenų apsaugos pareigūnas turi: b) ištirti teisinę aplinką, susijusią su socialinių tinklų duomenimis. Todėl remiantis šiais dviem būdais, pareigūnas gali bandyti nustatyti duomenų tvarkymo ribas. Kadangi nėra aiškių duomenų valdytojų gairių ir asmens duomenų tvarkymo taisykių socialiniuose tinkluose, tai sukuria terpę pareigūnui ieškoti panašių analogijų, kad sukurtų duomenų tvarkymo reikalavimus socialiniams tinklams[167].

3.4 Teisė būti pamirštam

Informacijos talpinimas internete socialinių tinklų laikais lėmė tai, kad prarandama asmeninių duomenų kontrolė. Ypatingas dėmesys šiame kontekste yra skiriamas paieškos sistemoms (pvz., *Google*), kadangi jų duomenų bazė padeda gauti informaciją apie asmenis paskelbtą internete, nepriklausomai nuo to ar ji vis dar aktuali, teisinga ir palanki konkrečiam asmeniui. Suprantama, kad tokios informacijos atvirumas gali neigiamai paveikti žmonių privatumą ar reputaciją[168].

Mokslininkas A. Montelero laikosi pozicijos, kad duomenų subjekto teisė būti pamirštam yra grindžiama fundamentaliu asmens poreikiu savarankiškai apsispręsti dėl savo gyvenimo, be nuolatinio pasmerkimo dėl savo paties praeities įvykių, ypatingai, kai tokie veiksmai buvo įvykę prieš ilgą laiką ir neturi jokio sąryšio su dabartiniu kontekstu[169]. Kiekvienas asmuo turėtų žinoti, kas ir kokiais tikslais renka jo duomenis,

---

[166] 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.

[167] OLSON, Cody. Effectively utilizing publicly accessible social media data while staying DGPR compliant, 2018. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga internete: https://www.finextra.com/blogposting/16206/effectively-utilizing-publicly-accessible-social-media-data-while-staying-gdpr-compliant>.

[168] VAN HOBOKEN, Joris. *Search engine freedom. On the implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Information Law Series 27, Alphen aan den Rijn: Kluwer Law International 2012, p. 99.

[169] MANTELERO, Alessandro. *The EU Proposal for a General Data Protection Regulation and the roots of the „right to be forgotten*. Elsevier: Computer law and Security review 29, 2013, p. 229-235.

kaip jie tvarkomi ir kiek ilgai saugomi, kad galėtų tuos duomenis tinkamai kontroliuoti[170]. Galimybės kontroliuoti savo duomenis didinimas pasireiškia tokių teisių visuma, kaip teisė susipažinti su savo duomenimis, juos ištaisyti, ištrinti, apriboti ar sustabdyti jų tvarkymą. Asmens turima kontrolė savo duomenims, būtų didinama laikantis duomenų kiekio mažinimo principo. Tai reikštų, kad duomenų valdytojai galėtų tvarkyti asmens duomenis tik numatytais tikslais[171].

Duomenų apsaugos reglamentas numato, kad asmens duomenys turi būti tikslūs, teisingi, išsamūs ir, jei būtina, nuolatos atnaujinami, atsižvelgiant į tikslą, dėl kurio jie yra saugomi. Šis principas įtvirtintas ir Europos Žmogaus Teisių Teismo jurisprudencijoje[172].

Teisė būti pamirštam,visų pirma, reglamentuoja ištrynimo įsipareigojimus. Pagal tai, asmens duomenys turi būti nedelsiant ištrinti, jei duomenys nebėra reikalingi jų pirminiam tvarkymo tikslui, arba duomenų subjektas atšaukė savo sutikimą ir nėra kito teisinio pagrindo tvarkyti, duomenų subjektas prieštaravo ir nėra duomenų, dėl svarbių teisėtų priežasčių tvarkyti, arba ištrinti reikalaujama, kad būtų laikomasi įstatymų nustatytų įpareigojimų pagal ES teisę arba valstybių narių teisę. Be to, duomenys, be abejonės, turi būti ištrinti, jei pats duomenų tvarkymas prieštarauja Reglamentui. Todėl teisė būti pamirštam yra grindžiama asmens autonomijos principu, kai tik pats individas gali spręsti dėl savo informacijos naudojimo. Teisė būti pamirštam, bendrąja prasme, įgalina duomenų subjektus gauti prieigą bei ištrinti asmeninius duomenis, renkamus trečiųjų asmenų, o taip pat, tam tikrais atvejais ir apriboti prieigą prie savo duomenų, paskelbtų internete[173].

Jei duomenų valdytojas asmeninius duomenis paskelbė viešai ir, jei yra viena iš pirmiau minėtų priežasčių, jis privalo imtis pagrįstų priemonių, atsižvelgdamas į minėtas aplinkybes, informuoti visus kitus duomenų valdytojus duomenų tvarkymo srityje, kad visos nuorodos į šiuos asmens duomenis, taip pat asmens duomenų kopijos ar kopijos turi būti ištrintos[174].

---

[170] Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM (2010) 609 galutinis, 2010, Briuselis, p. 5-17.

[171] Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamento pagrindai XXI amžiuje. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM (2012) 9 galutinis, 2012, Briuselis, p. 2.

[172] Europos Žmogaus Teisių Teismas. 2000 m. gegužės 4 d. sprendimas *Rotaru prieš Romuniją* byloje, Nr. 28341/95.

[173] AMBROSE, Meg Leta. Its about time: privacy, information life cycles, and the right to be forgotten. Stanford technology law review 16, 2, 2013, p. 385.

[174] 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.

Teisė būti pamirštam dėmesio sulaukė 2014 m. ES Teisingumo Teismo sprendime *Google Spain*, kuriame nustatė, jog paieškos variklio eksploatuotojas privalo iš rezultatų sąrašo, rodomo atlikus paiešką pagal asmens asmenvardį, pašalinti nuorodas iš trečiųjų asmenų paskelbtų tinklalapių, kuriuose yra informacijos apie šį asmenį, taip pat tais atvejais, kai šis asmenvardis arba ši informacija nėra prieš tai ištrinti arba tuo pat metu ištrinami iš šių tinklalapių, ir tai padaryti net jei atitinkami duomenys šiuose tinklalapiuose paskelbti teisėtai. Pagal Bendrojo duomenų apsaugos reglamento 17 straipsnį teisė būti pamirštam naudojamasi, pateikiant reikalavimą ištrinti duomenis, kurie nebėra reikalingi, kad būtų pasiekti tikslai, kuriais jie buvo renkami arba kitaip tvarkomi. Vadovaujantis ES Teisingumo Teismo *Google Spain* sprendime išdėstytais principais, šiomis teisėmis duomenų subjektas gali naudotis bet kokio duomenų valdytojo atžvilgiu, nepriklausomai nuo to, ar šie duomenys buvo gauti tiesiogiai iš to duomenų subjekto ar iš kito duomenų valdytojo, nepriklausomai nuo duomenų valdytojo atliekamo duomenų tvarkymo tikslo ir nepriklausomai nuo to, kad duomenų subjektas savo teise yra anksčiau naudojęsis kito duomenų valdytojo atžvilgiu. Be to, duomenis ištrinti gali būti reikalaujama ne tik duomenų subjektui pateikiant tiesioginį reikalavimą privačiam duomenų valdytojui, to reikalauti gali ir priežiūros ar teisminė institucija[175]. Svarbu ir tai, kad byloje *Google Spain* kalbėta tik apie paieškos sistemą. Dabar vienas pagrindinių pasikeitimų yra tai, kad galimybė būti pamirštam numatyta ne tik paieškos sistemose, tačiau ir apskritai[176].

Todėl svarbu paminėti, kad teisė būti pamirštam yra taikoma ir socialiniams tinklams. Ankščiau galiojusioje ,,Facebook" privatumo politikoje, vartotojui nebuvo galimybės išsitrinti savo paskyrą. Jei vartotojas nuspręsdavo, jog nebenori naudotis socialiniu tinklu Facebook, jam būdavo suteikta galimybė tik deaktyvuoti savo paskyrą. Tokiu atveju visa informacija, susijusi su vartotoju, paslepiama, tačiau neištrinama. Deaktyvavus paskyrą, kiti vartotojai nebegali susisiekti su vartotoju, ar peržiūrėti bendrintų nuotraukų, būsenų atnaujinimo ir pan. Nusprendus sugrįžti į socialinį tinklą, vartotojui tereikia įvesti buvusį slaptažodį ir Facebook atkuria visa informaciją, susijusią su vartotoju. Socialinis tinklas ,,Facebook", atnaujinęs privatumo politiką, suteikė galimybę asmenims išsitrinti savo vartotojo paskyrą. Tai atvejai, kai ,,Facebook" ištrina visą informaciją, kurią vartotojas buvo patalpinęs, pavyzdžiui, nuotraukas, video. Tačiau ,,Facebook" nurodo, jog ne visi duomenys yra ištrinami. ,,Facebook" pagalbos centro

[175] Europos Sąjungos Taryba. Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. Teisė būti pamirštam ir Teisingumo Teismo sprendimas dėl ,,Google" Politiniai debatai, Briuselis, 2014.

[176] POST, Robert. Data privacy dignitary privacy: Google Spain, The right to be forgotten, and the construction of the public sphere, 2018, p 982-1072.

puslapyje teigiama, kad tam tikros medžiagos kopijos (pavyzdžiui, prisijungimo įrašai) gali likti „Facebook" duomenų bazėje, tačiau visa ši informacija yra atskirta nuo asmeninių identifikatorių[177].

Reglamento 17 straipsnyje išdėstytos teisės nėra absoliučios – jos veikiau turi būti vertinamos atsižvelgiant į konkuruojančias teises ir konkuruojančius interesus. Savo sprendime Teisingumo Teismas pabrėžia, kad asmens duomenų tvarkymo, kai to reikia dėl teisėtų interesų, kurių siekia duomenų valdytojas – kaip yra paieškos variklio atveju – atžvilgiu reikia pasverti atitinkamas teises ir atitinkamus interesus, prieštaraujančius vienas kitam. Kadangi naudojimasis teise reikalauti ištrinti asmens duomenis galėtų turėti poveikio teisėtam interneto naudotojų, kurie gali būti suinteresuoti turėti prieigą prie tos informacijos, interesui, reikia nustatyti visų pirma teisingą to intereso ir Chartijos 7 bei 8 straipsniuose įtvirtintų duomenų subjekto pagrindinių teisių pusiausvyrą. Be to, ES Teisingumo Teismas konstatavo, kad nors šiuose straipsniuose įtvirtintos duomenų subjekto teisės paprastai yra viršesnės ir už šių vartotojų interesus, ši pusiausvyra konkrečiais atvejais gali priklausyti nuo atitinkamos informacijos pobūdžio ir jos ypatingumo duomenų subjekto privačiam gyvenimui, taip pat nuo visuomenės intereso gauti prieigą prie šios informacijos, nelygu, kokia šio asmens padėtis viešajame gyvenime[178].

Visgi būtina pastebėti, kad pirmiau minima teisė pagal prigimtį nėra absoliuti, o taikoma tik tuomet, jei asmeninė informacija duomenų apdorojimo tikslais yra netiksli, neadekvati, nereikšminga ar perteklinė. Tai taip pat reiškia, kad net tikslių duomenų teisėtas apdorojimas ilgainiui gali nebeatitikti duomenų apsaugos principų. Negana to, teisė būti pamirštam gali būti apribota esant bent vienai iš šių aplinkybių, nepriklausomai nuo to, ar šia teise siekia pasinaudoti asmuo, sąmoningai sutikęs dėl duomenų tvarkymo: nelaikytini atvejai Bendrojo duomenų apsaugos reglamento pažeidimu, kai asmens duomenys ir toliau saugomi, jei tai būtina pasinaudoti saviraiškos teise, informacijos laisve, siekiant įvykdyti teisinę prievolę, atlikti užduotį, vykdomą dėl viešojo intereso arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, dėl viešojo intereso priežasčių visuomenės sveikatos srityje, archyvavimo tikslais viešojo intereso

[177] Facebook privatumo politika. [Interaktyvus. Žiūrėta 2019 m. rugsėjo 12 d.] Prieiga per internetą: https://www.facebook.com/help/224562897555674.
[178] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain prieš Agencia Española de Protección de Datos* C-131/12, EU:C:2014:317, 81 punktas.

labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, arba siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus[179].

Praktikoje kiekvienas asmens pateiktas prašymas vertinamas atskirai, nes teisė būti pamirštam nebūtinai yra viršesnė už kitas pagrindines teises (pavyzdžiui, visuomenės interesą gauti tam tikrą informaciją, kuris gali būti viršesnis, kai asmuo yra, pavyzdžiui, viešas asmuo). Dėl to tarp įvairių teisių reikia ieškoti teisingos pusiausvyros.

Naujasis reglamentas taip pat perkelia įrodymų naštą nuo duomenų subjekto duomenų valdytojui. Tai reiškia, kad teisinį pagrindą prieštaravimui turi pateikti ne duomenų subjektas, o duomenų valdytojas – jis turi pateikti įtikinamą teisinį pagrindą duomenų apdorojimui, kuris yra viršesnis už duomenų subjekto interesus, teises ir laisves.

Darant išvadą galima patvirtinti, jog Bendrajame duomenų apsaugos reglamente numatyta teisė būti pamirštam turėtų palengvinti gyvenimą asmenims, numatant aplinkybes, kurių pagrindu galima reikalauti pašalinti duomenis, tačiau praktinė šios teisės pusė turėtų atsiskleisti vėliau. Taip pat socialinio tinkle „Facebook" privatumo politikos analizė leidžia daryti išvadą, jog pradėjus taikyti Bendrąjį duomenų apsaugos reglamentą, socialiniai tinklai įgalino teisę būti pamirštam, suteikiant galimybę vartojams išsitrinti paskyras. Tačiau kyla abejonių, ar tokia privatumo politika, kai socialiniam tinklui ištrinant tik tokią informaciją, kurią patalpino pats vartotojas, paliekant informaciją, kurią socialinis tinklas sukaupė remdamasis vartotojo atliktais veiksmais, pilnai išpildo Bendrajame duomenų apsaugos reglamente numatytą teisę.

[179] 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.

IŠVADOS

1. Globalizacija bei spartus technologijų vystymasis paskatino imtis priemonių, susijusių su socialinių tinklų saugumu. Kadangi apie socialiniuose tinkluose kylančias rizikas pastebėta neseniai, todėl teisės šaltinių, reguliuojančių socialinus tinklus nėra daug. Reikšmingiausiu socialinius tinklus reguliuojančiu šaltiniu reikėtų laikyti Bendrąjį duomenų apsaugos reglamentą, kuriame numatytos naujovės privertė socialinius tinklus atnaujinti privatumo politikas, siekiant tinkamos duomenų apsaugos.
2. Asmens duomenimis galima laikyti bet kokią informaciją, kurią galima susieti su konkrečiu asmeniu. Kadangi socialinių tinklų svetainėse asmens duomenų rinkimo būdai tapo gerokai sudėtingesni ir sunkiau atsekami, iškilo poreikis asmens duomenis apsaugoti, taikant Bendrąjį duomenų apsaugos reglamentą. Socialinio tinklo „Facebook" privatumo politikoje pateikiamas išsamus sąrašas tvarkomų asmens duomenų**,** tačiau trūksta išsamios informacijos, kaip yra tvarkomi specialių kategorijų asmens duomenys, kurie gauti iš trečiųjų šalių.
3. Visais atvejais socialinis tinklas „Facebook" reikalauja, kad duomenų subjektas (vartotojas) sutiktų su visa privatumo politika. Tam, kad asmens duomenų tvarkymas būtų laikomas teisėtu turi būti gautas asmens sutikimas ar kitas teisėtas pagrindas. Socialinio tinklo vartotojo sutikimas negalioja, kadangi vartotojas neturi realaus pasirinkimo, o nesutikęs su privatumo politika, negalėtų naudotis socialinio tinklo paslaugomis. Kai vartotojai privalo duoti sutikimą, kad galėtų naudotis socialinių tinklų paslaugomis, nėra laikoma savanorišku sutikimu, pagal Bendrąjį duomenų apsaugos reglamentą, todėl socialinio tinklo „Facebook" numatytas duomenų tvarkymo pagrindas yra neteisėtas.
4. Bendruoju duomenų apsaugos reglamentu įtvirtintas atskaitomybės principas sustiprina duomenų valdytojų atsakomybę už duomenų apsaugos teisės reikalavimų laikymąsi. Duomenų valdytojui kyla pareiga įrodinėti atitiktį duomenų apsaugos teisei, taip pat įvesta nauja pareiga atlikti poveikio duomenų apsaugai vertinimą, bei paskirti duomenų apsaugos pareigūną. Socialinių tinklų „Facebook" bei „Instagram" privatumo politikose nėra konkrečiai įvardinta, kas yra duomenų valdytojas. Tačiau ES Teisingumo Teismas išaiškino, kad duomenų valdytojo pozicija socialinių tinklų kontekste gali skirtis, dažniausiai duomenų valdytoju yra laikomas socialinis tinklas, tačiau galimi atvejai, kai egzistuoja bendri duomenų valdytojai – socialinis tinklas ir paskyrą turinti organizacija.

5. Atskaitomybės principas įpareigojo socialinius tinklus įvardinti kaip ir kokie konkretūs asmens duomenys yra renkami. Padidėjęs skaidrumo reikalavimas padidino informacijos prieinamumą socialinio tinklo „Facebook" vartotojams ir užtikrino vartotojų teisę gauti informaciją, apie su juo susijusius procesus. Tačiau socialinio tinklo „Facebook" privatumo politikos analizė parodė, kad socialinis tinklas duomenų apsaugos principus išpildo vien formaliai, kadangi privatumo politikose informacija, susijusi su duomenų tvarkymu išliko neaiški bei sunkiai prieinama, nėra nurodoma, kokios apimties asmens duomenys yra tvarkomi, bei nenurodoma kiek laiko asmens duomenys yra ar bus saugomi socialiniame tinkle.

LITERATŪROS IR KITŲ ŠALTINIŲ SĄRAŠAS

Norminiai teisės aktai

1. Lietuvos Respublikos Konstitucija. Valstybės žinios, 1992, nr. 33-1014.
2. Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*. 2006, Nr. 68-2497.
3. 1950 m. lapkričio 4 d. Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija. Valstybės žinios, 1995-05-16, Nr. 40-987.
4. 1981 m. sausio 28 d. Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (Konvencija Nr. 108). Valstybės žinios, 2001-04-13, Nr. 32-1059.
5. Europos Sąjungos pagrindinių teisių chartija. OL C 326, 2012 10 26, p. 391-407.
6. 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.
7. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL 2004 m. specialusis leidimas, 13 skyrius, 15 tomas, p. 355–374.
8. 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.
9. Valstybinė duomenų apsaugos inspekcija. *Asmens duomenų teisinės apsaugos įstatymo komentaras*. Vilnius, 2005, p. 25.

Specialioji literatūra

10. ABDESSLEM, Fehmi Ben et al. Reliable online social network data collection. Springer: Computational Social Networks: Mining and Visualization (2012): 183-202.
11. AMBROSE, Meg Leta. Its about time: privacy, information life cycles, and the right to be forgotten. Stanford technology law review 16, 2, 2013, p. 385.
12. AZUCAR, Danny. et al. Predicting the Big 5 Personality Traits from Digital Footprints on Social Media: A Meta-Analysis. *Personality and Individual Differences,* Vol. 124, 2018.

13. BOYD, Danah. ir ELLISON, Nicole. Social Network Sites: Definition, History, and Scholarship. *Journal of Computer-Mediated Communication* 13 (2007), p. 210-230.
14. BUCCAFURRI, Francesco et al. A model to support design and development of multiple-social-network applications. Elsevier: Information Sciences 331 (2016): 107.
15. CATE, H. Fred. *Privacy in the information age*. 1997. [interaktyvus. Žiūrėta 2019 m. kovo 5 d.]. Prieiga per internetą: http://brookings.nap.edu/books/0815713169/32.gif.
16. CIVILKA, Mindaugas; ŠLAPIMAITĖ, Lina. Asmens duomenų samprata elektroninėje erdvėje. Teisė, 2015, t. 96..
17. CIVILKA, Mindaugas., et al. *Informacinių technologijų teisė*. Vilnius: NVO Teisės institutas, 2004.
18. DE HERT, Paul et al. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law and Security Review, 2017.
19. DE HERT, Paul; CZERNIAWSKI, Michal. Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context. International Data Privacy Law, Volume 6, Issue 3, 2016;
20. DE HERT, Paul;PAPAKONSTANTINOU, Vagelis; The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. *Computer Law& Security Review 30* (2014) 633-642.
21. FELT, Adrienne. ir EVANS, David.Privacy protection for social networking APIs. Web 2.0 Security and Privacy , 2008: 1-9;
22. FLORIDI, Luciano. *Information a very short introduction*. Oxford University Press, 2010, p. 1.
23. YOUYOU, Wu. et al. Computer-Based Personality Judgments Are More Accurate Than Those Made by Humans. *Proceedings of the National Academy of Sciences USA*, Vol. 112, No. 4, 2015. [interaktyvus. Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: < http://www.richardbenjamintrust.co.uk/uploads/finalreports/2013/DStillwell.pdf>.
24. KELLEHER, Denis., MURRAY, Karen. *IT Law in the EU*. Sweet and Maxwell, 1999.

25. KUCZERAWY, Aleksandra. ir FANNY, Coudert. Privacy Settings in Social Networking Sites: Is It Fair?*. Interdisciplinary Centre for Law & ICT (ICRI) – K.U.Leuven - IBBT, Sint-Miechielsstraat 6, 3000 Leuven, Belgum.
26. KUNER, Christopher. European Data Protection Law and International Jurisdiction on the Internet (Part 1)18 International Journal of Law and Information Technology 176, 2010.
27. LAURENT, Maryline, ir LEVALLOIS-BARTH, Claire. Privacy Management and Protection of Personal Data. Digital Identity Management, 2015.
28. MALINAUSKAITĖ, I. *Privatumas socialiniuose tinkluose kaip įstatymo saugoma vertybė*. Social Transformations in Contemporary Society, 2015.
29. MALINAUSKAITĖ- VAN DE CASTEL, Inga. Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Mykolo Romerio universitetas, 2017.
30. MANTELERO, Alessandro. The EU Proposal for a General Data Protection Regulation and the roots of the ,,right to be forfotten. Elsevier: Computer law and Security review 29, 2013, p. 229-235.
31. MARTIN, Aaron. ir VAN BAVEL, Rene. Assesing the Benefits of Social Networks for Organizations (European Commision Joint research Center, 2013).
32. MOORE, Nick. *Rights and Responsibilities in an Information Society*// The Journal of Information Law and Technology. No1.1998. [interaktyvus. Žiūrėta 2019 m. kovo 5 d.]. Prieiga per internetą: http://elj.warwick.ac.uk/jilt/infosoc/1998_1moor/.
33. MOEREL, Lokke. The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide? 1 International Data Privacy Law 28, 2011.
34. OLSON, Cody. Effectively utilizing publicly accessible social media data while staying DGPR compliant, 2018. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga internete: https://www.finextra.com/blogposting/16206/effectively-utilizing-publicly-accessible-social-media-data-while-staying-gdpr-compliant.
35. PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2017, t. 80.
36. PETRAITYTĖ, Ilona. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
37. POST, C. Robert. Data privacy dignitary privacy: Google Spain, The right to be forgotten, and the construction of the public sphere, 2018, p 982-1072.

38. SCAIFE, Laura. *Handbook of Social Media and the law*. Informa Law from Routledge; 1 edition, 2015, p. 277.
39. SWEENEY, Latanya. Uniqueness of Simple Demographics in the U.S. Population. Technical report, Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA, 2000.
40. ŠTAREIKĖ, Eglė. ir KAUSTEKELYTĖ-TUNKEVIČIENĖ, Sigita. Pagrindinės duomenų subjekto teisės ir jų užtikrinimas pagal ES Bendrąjį duomenų apsaugos reglamentą. Mokslinių straipsnių rinkinys, Visuomenės saugumas ir viešoji tvarka, 2018.
41. ZALESKIS, Julius. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES bendrąjį duomenų apsaugos reglamentą. Teisė, 2017, t. 104.
42. ZALESKIS, Julius. ES Bendrasis duomenų apsaugos reglamentas: reikšmė duomenų apsaugos teisei. Teisė, 2017, t. 103.
43. ZALESKIS, Julius. Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė. VĮ Registrų centras, Vilnius, 2019.
44. VAN HOBOKEN, Joris. *Search engine freedom. On the implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines*, Information Law Series 27, Alphen aan den Rijn: Kluwer Law International 2012, p. 99.
45. WESTIN, Alan. Privacy and Freedom. *Washington and Lee Law Review* 1, 20, 1967.

Teismų šaltiniai

46. Lietuvos Respublikos Konstitucinio Teismo 2008 m. sausio 22 d. nutarimas „Dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Priėmimo į valstybės tarnautojo pareigas tvarkos patvirtinimo“ (2002 m. birţelio 24 d., 2002 m. rugpjūčio 29 d., 2003 m. birţelio 3 d., 2003 m. lapkričio 25 d., 2005 m. spalio 28 d. redakcijos) patvirtintos Priėmimo į valstybės tarnautojo pareigas tvarkos atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos įstatymo 3 straipsnio (2002 m. balandţio 23 d. redakcija) 1 daliai, dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2006 m. birţelio 28 d. redakcija) patvirtinto Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos

įstatymo 3 straipsnio (2002 m. balandţio 23 d., 2007 m. birţelio 7 d. redakcijos) 1 daliai, taip pat dėl Lietuvos Respublikos Vyriausybės 2002 m. birţelio 24 d. nutarimu Nr. 966 „Dėl Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2007 m. rugsėjo 26 d., 2007 m. gruodţio 12 d. redakcijos) patvirtinto Konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties Lietuvos Respublikos Konstitucijai, Lietuvos Respublikos valstybės tarnybos įstatymo 3 straipsnio (2007 m. birţelio 7 d. redakcija) 1 daliai“. Valstybės ţinios. 2008, Nr. 10-350.

47. Europos žmogaus teisių teismo 1992 m. gruodžio 16 d. sprendimas *Niemietz v. Germany,* Nr. 13710/88.
48. Europos žmogaus teisių teismo 1985 m. kovo 26 d. sprendimas *X and Y v. Netherlands,* Nr. 8978/80.
49. Europos Žmogaus Teisių Teismas. 2000 m. gegužės 4 d. sprendimas *Rotaru prieš Romuniją* byloje, Nr. 28341/95.
50. Europos Sąjungos Teisingumo Teismas. 2003 m. lapkričio 6 d. sprendimas *Bodil Lindqvist* byloje C-101/01, EU:C:2003:596.
51. Europos Sąjungos Teisingumo Teismas. 2003 m. kovo 6 d. sprendimas *Interporc Im, Export GmbH v. Komisija* C-41/00, EU:C:2003:125.
52. Europos Žmogaus Teisių Teismas. Teismas 2008 m. gruodžio 4 d. sprendimas *S. ir Marper prieš Jungtinę Karalystę,* Nr. 30562/04, 30566/04, §78-86.
53. Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain SL* ir *Google Inc* prieš *Agencia Española de Proteccion Datos (AEPD) ir Mario Costeja Gonzalez* C-131/12, EU:C:2014:317.
54. Europos Sąjungos Teisingumo Teismas. 2014 m. gruodžio 11 d. sprendimas *Ryneš prieš Úřad pro ochranu osobních údajů,* C-212/13, EU:C:2014:2428.
55. Europos Sąjungos Teisingumo Teismas. 2018 m. birželio 5 d. sprendimas *Wirtschaftsakademie Schleswig-Holstein GmbH* C-210/16, EU:C:2018:388.
56. Dutch-speaking court of first instance Brussels. 2015 m. lapkričio 9 decision Facebook Inc. prieš Facebook Belgium SPRL. , Nr. 584.[žiūrėta 2019 m. balandžio 12 d.] Prieiga per internetą: https://www.dataprotectionauthority.be/sites/privacycommission/files/documents/Judgement%20Belgian%20Privacy%20Commission%20v.%20Facebook%20-%2009-11-2015.pdf

***Soft law* šaltiniai**

57. ES 29 str. darbo grupė. *2009 m. birželio 12 d. Nuomonė 5/2009 dėl internetinių socialinių tinklų*, Nr. WP 163.
58. ES 29 str. darbo grupė. *2016 m. gruodžio 13 d. Gairės dėl duomenų apsaugos pareigūnų (DAP), Nr. WP 243*. [interaktyvus. Žiūrėta 2019 m. balandžio 5 d.]. Prieiga per internetą: <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf>.
59. ES 29 str. darbo grupės 2014 m. balandžio 9 d. Nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 straipsnį Nr. WP217. [interaktyvus. Žiūrėta 2019 m. spalio 20 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_lt.pdf>.
60. Article 29 Data Protection Working Party. *Opinion 3/2010 on the principle of accountability*. 00062/10/EN WP 173, p, 3.
61. 29 str. Darbo grupės 2011 m. liepos 13 d. Nuomonė dėl sąvokos „sutikimas" apibrėžties Nr. WP187. [interaktyvus; žiūrėta 2019 m. spalio 21 d.]. Prieiga per internetą: <https://www.pdpjournals.com/docs/88081.pdf>.
62. ES 29 str. darbo grupės 2007 m. birželio 20 d. nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136, p. 6. [interaktyvus; Žiūrėta 2019 m. lapkričio 10 d.]. Prieiga per internetą: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf.
63. ES 29 str. darbo grupė. 2017 m. spalio 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, WP 248 rev. 01, p. 9-11.
64. Proposals for Amendments regarding exemption for personal or household activities. Annex 2. The situation under Directive 95/46/EC.
65. Europos Komisija. Dėl asmens duomenų perdavimo iš ES į Jungtines Amerikos Valstijas pagal Direktyvą 95/46/EB, Teisingumo Teismui priėmus sprendimą byloje C-362/14 (Schrems). *Komisijos komunikatas Europos Parlamentui ir Tarybai COM(2015) 566 galutinis*, 2015, Briuselis, p. 4.

66. ENISA Position Paper No. 1 *Security Issues and Recommendations for Online Social Networks*. October 2007.
67. Ekonominio bendradarbiavimo ir plėtros organizacijos informacijos saugumo ir privatumo darbo grupė. Inventory of instruments and mechanisms, contributing to the implementation and enforcement of the OECD Privacy Guidelines on Global Networks, Paris, 1999, p. 10 [interaktyvus. Žiūrėta 2019 m. Balandžio 3 d.] prieiga per internetą: http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/REG(98)12/FINAL &docLanguage=En.
68. Europos Komisija. Visapusiškas požiūris į asmens duomenų apsaugą Europos Sąjungoje. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM (2010) 609 galutinis, 2010, Briuselis, p. 5-17.
69. Europos Komisija. Privatumo apsauga glaudžiai susijusiame pasaulyje: Europos duomenų apsaugos reglamento pagrindai XXI amžiuje. Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui COM (2012) 9 galutinis, 2012, Briuselis, p. 2.
70. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, 2018. [interaktyvus. Žiūrėta 2019 m. kovo 26 d.]. Prieiga per internetą: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_3_2018_territorial_scope_en.pdf.

Kiti šaltiniai

71. Airbnb. *Terms of Service* [interaktyvus. Žiūrėta 2018-02-28]. Prieiga per internetą: <https://www.airbnb.com/terms/>.
72. Facebook. *Terms of service. Section 3* [interaktyvus. Žiūrėta 2019-02-28]. Prieiga per internetą: <http://www.facebook.com/legal/terms>.
73. SCHECHNER, Sam. You Give Apps Sensitive Personal Information. Then They Tell Facebook. [interaktyvus. Žiūrėta 2019-02-28]. Prieiga per internetą: https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636
74. Europos Sąjungos Taryba. Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo

tokių duomenų judėjimo. Teisė būti pamirštam ir Teisingumo Teismo sprendimas dėl „Google" Politiniai debatai, Briuselis, 2014.

75. BOSTON CONSULTING GROUP. *The Value of Our Digital Identy. Liberty Global*, Inc., 2012, p. 103 [interaktyvus. Žiūrėta 2019 m. kovo 10 d.]. Prieiga per internetą: <https://2zn23x1nwzzj494slw48aylw-wpengine.netdna-ssl.com/wp-content/uploads/2017/06/The-Value-of-Our-Digital-Identity.pdf>.
76. The Guardian. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, 2018 m. kovo 17 d. [Interaktyvus. Žiūrėta 2019 m. rugsėjo 10 d.]. Prieiga per internetą: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.
77. Complaint Under Article 77(1) DGPR. [interaktyvus. Žiūrėta 2019 m. lapkričio 22 d.]. Prieiga per internetą: <https://noyb.eu/wp-content/uploads/2018/05/complaint-facebook.pdf>.

SANTRAUKA

Šiais laikais, dėl globalizacijos bei naujų technologijų atsiradimo, kyla naujų asmens duomenų apsaugos sunkumų. Ženkliai išaugo asmens duomenų rinkimo ir keitimosi jais mastas, kadangi fiziniai asmenys viešina vis daugiau asmeninės informacijos internete. Socialiniai tinklai, dėl milžiniško vartotojų skaičiaus, tampa vieni didžiausių asmens duomenų valdytojų, kurie renka, saugo, tvarko ar kitaip naudoja vartotojų asmens duomenis. Todėl socialinių tinklų vartotojai turi teisėtą lūkestį, kad jų asmens duomenys būtų tvarkomi užtikrinant aukštą asmens duomenų apsaugos lygį. Siekis prisitaikyti prie vykstančių pokyčių, nulėmė poreikį ES domenų apsaugos teisės reformai - 2018 m. gegužės 25 d. pradėtas taikyti Bendrasis duomenų apsaugos reglamentas. Atsižvelgiant į Bendrojo duomenų apsaugos reglamento reikalavimus, svarbu atlikti tyrimą ar asmens duomenų apsauga socialiniuose tinkluose yra pakankama. Todėl šiame darbe siekiama išnagrinėti kaip Bendrasis duomenų apsaugos reglamentas taikomas socialiniams tinklams.

Pirmoje darbo dalyje pristatomas socialinių tinklų teisinis reguliavimas, išaiškinama socialinių tinklų samprata bei atskleidžiami duomenų apsaugos šaltiniai, reguliuojantys socialinius tinklus. Antra dalis skirta atskleisti Bendrojo duomenų apsaugos reglamento taikymą socialiniuose tinkluose. Todėl analizuojama asmens duomenų rinkimo problematika, nustatoma duomenų valdytojo pozicija socialiniuose tinkluose, bei išsiaiškinama, kokiais atvejais Bendrasis duomenų apsaugos reglamentas taikomas ne ES įsisteigusioms įmonėms. Be to, aptariami atvejai, kai Bendrasis duomenų apsaugos reglamentas netaikomas. Trečioje dalyje siekiant išsiaiškinti, kaip socialiniai tinklai įgyvendina Bendrojo duomenų apsaugos reglamento reikalavimus, analizuojamos populiariausių socialinių tinklų privatumo politikų nuostatos, dėl teisėto duomenų tvarkymo, duomenų apsaugos principų įgyvendinimo, teisės būti pamirštam bei pareigos paskirti duomenų apsaugos pareigūną.

SUMMARY

EU General Data Protection Regulation and social networks

Nowadays, due to globalization and the emergence of new technologies, new challenges are emerging for the protection of personal data. The scale of the collection and exchange of personal data has increased significantly, because natural persons increasingly make personal information available on the internet. Due to the huge number of users, social networks are becoming one of the largest personal data controllers who collect, store, process or otherwise use personal data of users. Therefore, social network users have a legitimate expectation that their personal data will be processed with a high level of protection of personal data. In order to adapt to ongoing changes, it has led to the need for EU data protection reform, on 25th of May 2018 the General Data Protection Regulation became applicable. Given the requirements of General Data Protection Regulation, it is important to investigate wheter personal data protection in social networks is sufficient. Therefore, this work aims to examine how the General Data Protection Regulation applies to social networks.

The first part introduces the legal regulation of social networks, analyzes the concept of social networks and reveals the data protection sources that regulate social networks. The second part is dedicated to reveal the application of the General Data Protection Regulation to social networks. Therefore, the analysis of personal data collection issues, the position of the controller in social networks and clarifies when non-EU companies are covered by the General Data Protection Regulation. In addition, it is discussed on which cases General Data Protection Regulation does not apply. The third section explores how social networks implement the requirements of the General Data Protection Regulation by analyzing the most popular social network privacy policies regarding lawful processing, implementation of data protection principles, the right to be forgotten, and the obligation to appoint a data protection officer.