

Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedra

Krystynos Gulbickaitės
II kurso, ES verslo teisės
programos studentė

Magistro darbas
ES bendrojo duomenų apsaugos reglamento taikymo socialiniams
tinklams ypatumai

Vadovas: asist. dr. Julius Zaleskis

Recenzentas: prof. dr. Vytautas Mizaras

Vilnius

2019

TURINYS

ĮVADAS	3
1.SOCIALINIŲ TINKLŲ KONCEPCIJA	6
1.1 Socialinių tinklų sąvoka	6
1.2 Socialinių tinklų veikimo modelis.....	9
1.3 Socialinių tinklų teigiamos ir neigiamos pasekmės	11
2.BDAR ASMENS DUOMENŲ APSAUGOS TAIKYMO RIBOS SOCIALINIAMS TINKLAMS	15
2.1 Asmens duomenų sąvokos analizė.....	15
2.2 Asmens duomenų apsaugos valdytojas ir tvarkytojas socialiniuose tinkluose	20
2.3 Privatumo santykis su asmens duomenimis virtualioje erdvėje.....	25
3. SOCIALINIŲ TINKLŲ PAREIGOS ASMENS DUOMENŲ APSAUGAI UŽTIKRINTI.....	30
3.1 Teisėtumo, sąžiningumo ir skaidrumo principas asmens duomenų apsaugoje	30
3.2 Duomenų tvarkymo tikslo apribojimo principo įgyvendinimas socialiniuose tinkluose	34
3.3 Duomenų kiekio mažinimo pareiga	37
3.4 Duomenų tikslumo principo privalomumas	42
3.5 Saugumo užtikrinimas ir atskaitomybės pareiga.....	45
3.6 Duomenų subjektų teisės ir duomenų apsaugos pareigūno vaidmuo.....	49
4. ASMENS DUOMENŲ APSAUGOS TEISĖS PAŽEIDIMAI SOCIALINIUOSE TINKLUOSE	54
4.1 Duomenų politikos socialiniuose tinkluose „Facebook“ ir „Instagram“ vertinimas pagal BDAR reikalavimus	54
4.2 Asmens duomenų teisės pažeidimai socialiniuose tinkluose naujausioje teismų praktikoje.....	61
4.3 Apklausos „Asmens duomenų apsauga socialiniuose tinkluose“ rezultatai	67
IŠVADOS	69
ŠALTINIŲ SĄRAŠAS	71
SANTRAUKA (lietuvių kalba)	79
SUMMARY (anglų kalba).....	80
PRIEDAS NR. 1 APKLAUSOS „ASMENS DUOMENŲ APSAUGA SOCIALINIUOSE TINKLUOSE“ REZULTATAI.....	81

IVADAS

Temos aktualumas. Socialiniai tinklai yra XXI amžiaus technologijų pažangos reiškiny, kuris pasižymi tiek teigiamais, tiek neigiamais aspektais. Socialiniai tinklai pagal Danah Boyd ir Nicole Ellison (2017)¹ apibrėžiami kaip internetinės paslaugos, leidžiančios asmenims 1) susikurti viešą ar pusiau viešą profilį apribotoje sistemoje, 2) sudaryti kitų vartotojų, su kuriais jie naudojami, sąrašą, ir (3) peržiūrėti ir apsilankyti jų ir kitų sistemos narių prisijungimų sąrašuose. Kitaip tariant socialiniai tinklai – tai virtuali erdvė, kur vartotojai susikuria asmeninius profilius, bendrauja su kitais žmonėmis taip pat dalinasi privačia informacija: nuotraukomis, vietomis, kur keliauja, kokiuose restoranuose lankosi. Šiais laikais sunku įsivaizduoti žmogų, neturintį socialinio tinklo, nes pasaulyje socialiniais tinklais naudojami milijardai žmonių, pavyzdžiui, šiame darbe bus analizuojamas „Facebook“ socialinis tinklas, kuriuo naudojami pagal naujausią statistiką² 2,4 milijardo žmonių. Skaičiai yra milžiniški ir duomenų apsauga yra neišvengiama mūsų vartotojiškoje visuomenėje, kurioje tiesioginės rinkodarais tikslais dažnai panaudojami asmens duomenys. Esant tokiam pavojui ir siekiant susitiprinti asmens duomenų apsaugą bei nustatyti teises ir pareigas asmenims tvarkantiems duomenis buvo priimtas 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 toliau - BDAR) pradėtas taikyti Lietuvoje nuo 2018 m. gegužės 25 d. Nauji reikalavimai nustatyti BDAR apima: organizacijos asmens duomenų tvarkymo taisykles ar privatumo politiką, duomenų subjekto sutikimą tvarkyti jo asmens duomenis, asmens amžiaus patikrinimo sistemas ir tėvų arba teisėtų atstovų sutikimą dėl nepilnamečių asmens duomenų tvarkymo, tinkamą asmens duomenų saugojimą, tvarkymą ir valdymą, asmens duomenų saugumo pažeidimus (aptikimą, pranešimą ir ištyrimą), duomenų subjekto prašymo dėl teisės susipažinti su savo asmens duomenimis įgyvendinimą, duomenų subjektų teises ir jų įgyvendinimą („teisė būti pamirštam“, duomenų perkeliamumas) ir pan.³ Šiame darbe bus analizuojami pagrindiniai reikalavimai duomenų valdytojams socialiniuose tinkluose ir duomenų subjektų teisių įgyvendinimas pagal BDAR.

¹ Danah Boyd ir Nicole Ellison publication history [interaktyvus, žiūrėta 2019 m. lapkričio 8 d.]. Prieiga per internetą: <<https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x>>.

² Statista tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 8 d.]. Prieiga per internetą: <<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>>.

³ GDPR tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 7 d.]. Prieiga per internetą: <<https://gdpr.lt/>>.

Darbo tikslas. Įvertinti, ar tinkamai socialiniai tinklai taiko BDAR užtikrindami asmens duomenų apsaugą.

Darbo uždaviniai.

1. Išanalizuoti, kokiems duomenims yra taikomas BDAR.
2. Nustatyti privatumo ir asmens duomenų santykį.
3. Atskleisti, kas yra duomenų valdytojai socialiniuose tinkluose ir kokios pareigos numatytos pagal BDAR.
4. Atlikti socialinių tinklų „Facebook“ platformos duomenų politikos analizę taikant BDAR numatytus reikalavimus.
5. Atlikti naujausios teismų praktikos apžvalgą dėl asmens duomenų apsaugos teisės pažeidimų „Facebook“ socialiniame tinkle.

Darbo objektas – socialinių tinklų asmens duomenų apsauga taikant BDAR. Konkrečiai bus analizuojamas „Facebook“ socialinis tinklas kaip pavyzdys darbo kontekste, nes šiandieninė teismų praktika asmens duomenų apsaugos aspektu yra nauja ir besiformuojanti. Esminiai BDAR teisės pažeidimai susiję su socialiniais tinklais aptikti tik „Facebook“ platformoje.

Tyrimo metodai. Šiame darbe daugiausiai naudojamas sisteminis tyrimo metodas analizuojant BDAR taip pat aktualiausią specialiąją literatūrą susijusią su asmens duomenų apsauga socialiniuose tinkluose – 2019 m. Juliaus Zaleskio monografija „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“, didelis dėmesys skirtas asmens duomenų apsaugos teisę aiškinančioms ES 29 str. darbo grupės nuomonėms, lyginamuoju metodu vertinama naujausia ES teismų praktika susijusi su „Facebook“ bei to pačio socialinio tinklo duomenų politika, istoriniu metodu apžvelgiama socialinių tinklų sąvokos istorija nuo atsiradimo iki šių dienų pokyčių.

Darbo originalumas. Šiame darbe nagrinėjamos BDAR nuostatos ir jų taikymas socialiniuose tinkluose. Kadangi BDAR įsigaliojo ir pradėtas taikyti neseniai – 2018 m. gegužės 25 d., todėl tokių tyrimų dėl asmens duomenų apsaugos socialiniuose tinkluose nėra atlikta labai daug. Asmens duomenų sąvoka nagrinėta 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvos (95/46/EB) (toliau – 95/46 direktyva) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo kontekste socialiniuose tinkluose 2015 m. Mindaugo Civilkos ir Linos Šlapimaitės straipsnyje „Asmens duomenų samprata elektroninėje erdvėje“, taip pat šios direktyvos kontekste buvo nagrinėtos duomenų subjektų teisės

2017 m. Ingos Malinauskaitė-Van de castel daktaro disertacijoje „Duomenų subjekto teisės virtualiuose socialiniuose tinkluose“ bei apžvelgta duomenų valdytojų atsakomybė socialiniuose tinkluose 2013 m. Gintarė Sirbikytės straipsnyje „Ar socialinio tinklo valdytojas atsako už šio tinklo naudotojo neteisėtai veiksmais padarytą žalą?“. Svarbu pabrėžti, kad minėti tyrimai atlikti 95/46 direktyvos kontekste, o remiantis BDAR nuostatomis tokių tyrimų nėra atlikta bei teismų praktika nėra analizuota iki šio darbo, nes reikšmingų išaiškinimų dėl duomenų valdytojo sąvokos išplėtimo ir duomenų tvarkymo socialiniuose tinkluose priimta 2016 m. – 2019 m. laikotarpiu.

Svarbiausi šaltiniai. Šiame darbe svarbiausi nagrinėjami šaltiniai yra BDAR⁴, ES 29 str. darbo grupės gairės dėl sutikimo⁵, dėl skaidrumo⁶, nuomonės dėl socialinių tinklų⁷, dėl duomenų valdytojo ir duomenų tvarkytojo sąvokų⁸, dėl asmens duomenų sąvokos⁹, Juliaus Zaleskio monografija dėl BDAR ir asmens duomenų apsaugos¹⁰, naujausia teismų praktika – bylos dėl duomenų valdytojo sąvokos socialiniame tinkle „Facebook“¹¹, dėl „Like“ mygtuko reikšmės nustatant duomenų valdytoją socialiniame tinkle „Facebook“¹² dėl mokymo vertinimo socialiniuose tinkluose¹³.

⁴ 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 2016 L 119, p.

[interaktyvus, žiūrėta 2019 m. rugsėjo 22 d.]. Prieiga per internetą: <<https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:32016R0679&from=lt>>.

⁵ 2017 m. lapkričio 28 d. ES 29 str. darbo grupės gairės dėl sutikimo pagal Reglamentą (ES) 2016/679 Nr. WP259 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą:

⁶ 2017 m. ES 29 str. darbo grupės gairės dėl skaidrumo [interaktyvus, žiūrėta 2019 m. spalio 18 d.]. Prieiga per internetą: <https://iapp.org/media/pdf/resource_center/wp29-transparency-12-12-17.pdf>.

⁷ 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>.

⁸ 2010 m. vasario 16 d. ES 29 str. darbo grupės nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP169 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.

⁹ 2007 m. birželio 20 d. ES 29 str. darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.

¹⁰ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registų centras, 2019.

¹¹ Europos Teisingumo teismas. 2018 m. birželio 5 d. sprendimas *Vokietijos regioninė duomenų apsaugos institucija prieš Vokietijos mokymo bendrovę GmbH* [interaktyvus, žiūrėta 2019 m. rugsėjo 16 d.]. Prieiga per internetą:

<<http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=LT>>.

¹² Europos Teisingumo teismas. 2019 m. liepos 12 d. byla *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Nr. C-40/17 [interaktyvus, žiūrėta 2019 m. lapkričio 3 d.]. Prieiga per internetą: <<https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf>>.

¹³ Lietuvos Vyriausiojo administracinio teismo teisėjų kolegija. 2016 m. birželio 13 d. *nutartis administracinėje byloje UAB „Creditinfo Lietuva“ v. Valstybinė duomenų inspekcija*, Nr. A-408-858/2016.

1.SOCIALINIŲ TINKLŲ KONCEPCIJA

1.1 Socialinių tinklų sąvoka

Prieš pradėdant analizuoti BDAR taikymą socialiniams tinklams, svarbu išnagrinėti bendrą kontekstą, kas yra socialiniai tinklai, kaip apibrėžiami ir kokius duomenis jie apima, taip pat svarbu įvertinti, kokie socialiniai tinklai yra šiandien bei kokie galimi pavojai duomenų apsaugai, ar apskritai, socialiniams tinklams reikalinga ir ar gali būti taikoma asmens duomenų apsauga numatyta BDAR. Tam išsiaiškinti, toliau bus analizuojama socialinių tinklų koncepcija, veikimo modelis, teigiamos ir neigiamos pasekmės šiuolaikiniame technologijų kontekste.

Socialiniai tinklai kaip sąvoka nėra paaiškinama vienu konkrečiu apibūdinimu, nes tai pakankamai naujas 2005-2007¹⁴ atsiradęs kintantis XXI amžiaus technologijų reiškinyš. Objektyviaja prasme vertinant funkcionalumo kriterijų, numatytą bei aiškinamą pagal informacinių technologijų mokslą – tai sąvokos visuma, sudaryta iš trijų elementų: fizinio, kodavimo bei aplikacijų. Fizinė prasme tinklo architektūra unikalios dizaino ir programavimo kalbos pagalba leidžia toli esančius vieną nuo kito įrenginius sujungti į globalų tinklų tinklą, vadinamą internetu. Kodavimo prasme, tinklo operacinės sistemos ir interneto naršyklės naudoja bendrą unikalią kalbą, vadinamą TCP/IP protokolu, kuris ir įgalina informacijos srautų tekėjimą tinkluose. Aplikacijų prasme, aukštesnio lygio protokolai, tokie kaip HTTP/ HTML, SMTP, VoIP, RTP yra kiekvieną dieną naudojami vartotojų skaityti internetinius tinklaraščius, skelbti atnaujinimus virtualiuose socialiniuose tinkluose kaip Facebook, Instagram, Twitter, naudotis Skype, ar siųsti audio ir video turinį.¹⁵ Subjektyviaja prasme, tai sociumas susibūręs virtualioje erdvėje, kurioje bendraujama, dalinamasi informacija ne tik apie save, bet ir apie visuomenėje vykstančius įvykius, naujienas, taip pat vykdoma komercinė veikla ir t.t. Socialinės medijos ir komunikacijos technologijų tyrinėtojos Danah Boyd ir Nicole Ellison (2007) apibrėžia socialinius tinklus kaip žiniatinklio paslaugas, suteikiančias vartotojams galimybes kurti savo viešą ar pusiau viešą profilį apibrėžtos sistemos ribose; formuoti kitų susijusių vartotojų sąrašą; peržiūrėti savo ir kitų tinklo vartotojų ryšių sąrašą.¹⁶ Teisine prasme socialiniai tinklai pagal ES 29 str darbo grupės 2009 m. birželio 12 d. priimtoje Nuomonėje

¹⁴ SIRBIKYTĖ, Gintarė. Ar socialinio tinklo valdytojas atsako už šio tinklo naudotojo neteisėtais veiksmais padarytą žalą? *Teisės apžvalga*, 2013, p. 30-85.

¹⁵ MALINAUSKAITĖ-VAN DE CASTEL, Inga. *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose*: daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2017.

¹⁶ SAVICKA, Aida. Virtualūs socialiniai tinklai: viešumo ir privatumo problematika. *Lietuvos kultūros tyrimai*. 2012, p. 157.

Nr. 5/2009 dėl socialinių tinklų internete¹⁷ socialinių tinklų paslauga apibūdinama kaip internetinė ryšių platforma, leidžianti žmonėms susisiekti arba kurti tų pačių pažiūrų vartotojų tinklus. Kaip nurodoma Nuomonėje, teisiniu požiūriu internetiniai socialiniai tinklai yra informacinės visuomenės paslaugos, kaip apibrėžta 1998 m. birželio 22 d. Europos Parlamento ir Tarybos direktyvos 98/34/EB, nustatančios informacijos apie techninius standartus ir reglamentus teikimo tvarką, iš dalies pakeistos 1998 m. liepos 20 d. Europos Parlamento ir Tarybos direktyva 98/48/EB, iš dalies keičiančia direktyvą 98/34/EB, nustatančią informacijos apie techninius standartus ir reglamentus teikimo tvarką 1 straipsnio 2 dalyje (dėl šiuo metu galiojančio apibrėžimo žr. 2015 m. rugsėjo 9 d. Europos Parlamento ir Tarybos direktyvos (ES) 2015/1535), kuria nustatoma informacijos apie techninius reglamentus ir informacinės visuomenės paslaugų taisykles teikimo tvarka, 1 straipsnio 1 dalies b punktą). Socialinių tinklų paslaugos turi panašių požymių: vartotojų prašoma pateikti asmens duomenis siekiant sukurti jų pačių aprašą arba profilį; socialinių tinklų paslaugų teikėjai taip pat teikia priemonių, leidžiančių vartotojams skelbti savo medžiagą (vartotojų kuriamą turinį, pvz., nuotraukas ar dienoraščio įrašą, muzikos ar vaizdo klipus arba nuorodas į kitas svetaines); socialinio darbo tinkle galimybė sukuriama naudojant priemones, kuriomis kiekvienam vartotojui pateikiamas adresatų sąrašas ir kuriomis naudodamasis vartotojas gali sąveikauti su kitais vartotojais. Svarbus privatumo nuostatų aspektas yra prieiga prie profilyje skelbiamų asmens duomenų. Jei tokiai prieigai netaikomi jokie apribojimai, trečiosios šalys gali susieti įvairią asmeninę informaciją, susijusią su vartotojais kaip socialinių tinklų paslaugų nariais arba per programines paieškos priemones. Socialinių tinklų paslaugų teikėjai turėtų pranešti vartotojams apie savo tapatybę ir įvairius tikslus, dėl kurių jie tvarko asmens duomenis pagal Duomenų apsaugos direktyvos (Direktyva 95/46/EB dabar galiojantis BDAR) 10 straipsnio nuostatas, įskaitant šią informaciją, bet ja neapsiribojant: duomenų naudojimą tiesioginės rinkodaros tikslais; galimą duomenų keitimąsi su nurodytų kategorijų trečiosiomis šalimis; profilių peržiūrą: jų kūrimą ir pagrindinius duomenų šaltinius; neskelbtinų duomenų naudojimą.¹⁸

Socialiniai tinklai kaip tokie atsirado iš besiburiančių bendruomenių internetinėje erdvėje. Pirmasis iš tokių buvo 1994 m. „www.geocities.com“, kurio esmė - leisti vartotojams kurti savo interneto svetaines, suskirstant jas į skirtingus „miestus“ pagal svetainės turinį. Po metų atsirado panašesnis į šiuolaikinius socialinius tinklus tinklas -

¹⁷ ES 29 str. darbo grupės 2009 m. birželio 12 d. Nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus. Žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

¹⁸ Lietuvos Vyriausiojo administracinio teismo teisėjų kolegija. 2016 m. birželio 13 d. nutartis administracinėje byloje UAB „Creditinfo Lietuva“ v. Valstybinė duomenų inspekcija, Nr. A-408-858/2016.

„TheGlobe.com“, kuris veiklą pradėjo viešai, suteikdamas vartotojams galimybę bendrauti su žmonėmis, turinčius pačius pomėgius bei leisdamas skelbti savo individualų turinį. 1997 m. sukurti „AOL Instant Messenger“ ir „SixDegrees.com“, kuriuose atsirado pirmieji „momentiniai“ pranešimai, suteikiantys vartotojams laisvę kalbėtis su draugais bei susikurti asmeninį profilį. AOL tikriausiai buvo tikras šių dienų socialinių tinklų svetainių pirmtakas. Narių profiliai leido vartotojams susikurti biografiją ir pasidalinti informacija apie save. Tuo metu sukurta inovatyviausia funkcija leido ieškoti kitų vartotojų profilių. Kitos svetainės sekė panašiu pavyzdžiu ir kūrėsi tokios socialinių tinklų svetainės kaip „Classmates“, „Friendzy“, „Hi-5“. Daugelis jų buvo pažinčių svetainės. Pvz., Klasiokai leido vartotojams susisiekti su senais klasės draugais. Šis socialinis tinklas susilaukė didžiulio susidomėjimo bei populiarumo, o šiandien klasės draugai vis dar turi apie 40 000 000 registruotų vartotojų. Šis dešimtmetis taip pat buvo sėkmingas ir „Yahoo“ bei „Amazon“ svetainėms, kuriomis naudojasi daug žmonių ne tik dėl bendravimo, bet ir komercinės veiklos.¹⁹ Labiausiai ir plačiausiai naudojamas socialinis tinklas šiandien yra 2004 m. amerikiečio Marko Zuckerbergo sukurtas „Facebook“, kuriuo kiekvieną dieną naudojasi 1.59 milijardo žmonių. Socialinių tinklų masinis paplitimas visuomenėje reiškia, kad kuo daugiau asmenų naudojasi socialinių tinklų paslaugomis, tuo labiau didėja duomenų subjekto teisių pažeidimų tikimybė²⁰. Skaičiai yra milžiniški, todėl informacijos taip pat yra daug bei kuo daugiau žmonių naudojasi, tuo didesnė rizika pažeisti teisę į privatumą, naudotis duomenimis rinkodaros tikslais be sutikimo ir t.t. Socialiniame gyvenime socialiniai tinklai yra paprasčiausios komunikacinės struktūros. Pavyzdžiui, anot P. R. Monge ir N. S. Contractor (2003: 3), komunikaciniai tinklai yra sąlyčio modeliai, kurie per pranešimų srautą laike ir erdvėje yra sukuriami komunikuojančiųjų. Pasak G. Kossinets ir kt. (2008: 435) socialiniai tinklai tarnauja kaip komunikacijos kanalai. Komunikacija sklinda per tinklus tarsi atskirų komunikacinių įvykių, tokių kaip susitikimai, tiesioginiai ar telefoniniai pokalbiai, elektroninio pašto ar tekstinės žinutės, rezultatas. H. Rheingold (1993: 58) detalizuoja: socialiniuose tinkluose mes kalbamės ir ginčijamės, įsitraukiame į intelektualų diskursą, vykdome komercinius veiksmus, keičiamės žiniomis, dalinamės emocijomis, planuojame, semiamės minčių, paskalų, nesantaikų, įsimylime,

¹⁹ The history of social networking: how it all began [interaktyvus, žiūrėta 2019 m. rugpjūčio 18 d.]. Prieiga per internetą:

<<https://1stwebdesigner.com/history-of-social-networking/>>

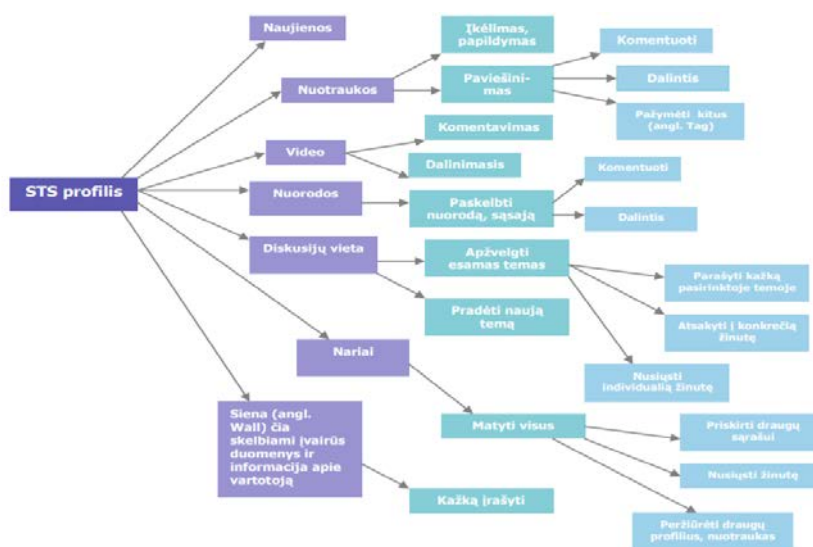
²⁰ MALINAUSKAITĖ-VAN DE CASTEL, Inga. *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose*: daktaro disertacija. Socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2017, p. 7.

susirandame draugų ir juos prarandame, žaidžiame žaidimus ir metažaidimus, flirtuojame.²¹

Taigi, socialinių tinklų sąvoka nuo pat jų atsiradimo pradžios buvo kintanti ir kuo toliau, tuo labiau išsiplėtė jos turinys asmens duomenų atžvilgiu, todėl ne veltui šiandien yra skiriamas didelis dėmesys asmens duomenų apsaugai socialiniuose tinkluose, kur duomenų srautai kiekvieną dieną vis didėja – vyrauja tiek privati informacija apie vartotojus komunikuojant, tiek komercinė veikla, rinkodara ir pan. Asmens duomenų saugumui užtikrinti teisiniu lygmeniu priimta nemažai teisės aktų, kurie bus analizuojami kitame skyriuje (nuo 2.), o prieš tai svarbu išanalizuoti socialinių tinklų veikimo modelį naudojant asmens duomenis.

1.2 Socialinių tinklų veikimo modelis

Šiuolaikiniai socialiniai tinklai veikia labai panašiai, dažnu atveju skiriasi tik pavaizdavimo būdas, išraiška, o esmė išlieka ta pati (žr. į 1 pav.) – kuo daugiau žmonių naudojami socialiniais tinklais, tuo daugiau sukuriama asmeninių profilių, dalinamasi naujienomis, nuotraukomis, video, diskutuojama su grupės nariais įvairiomis temomis pagal vartotojų poreikį. Tai reiškia, kad socialiniuose tinkluose sukaupiama nemažai asmens privačių duomenų.



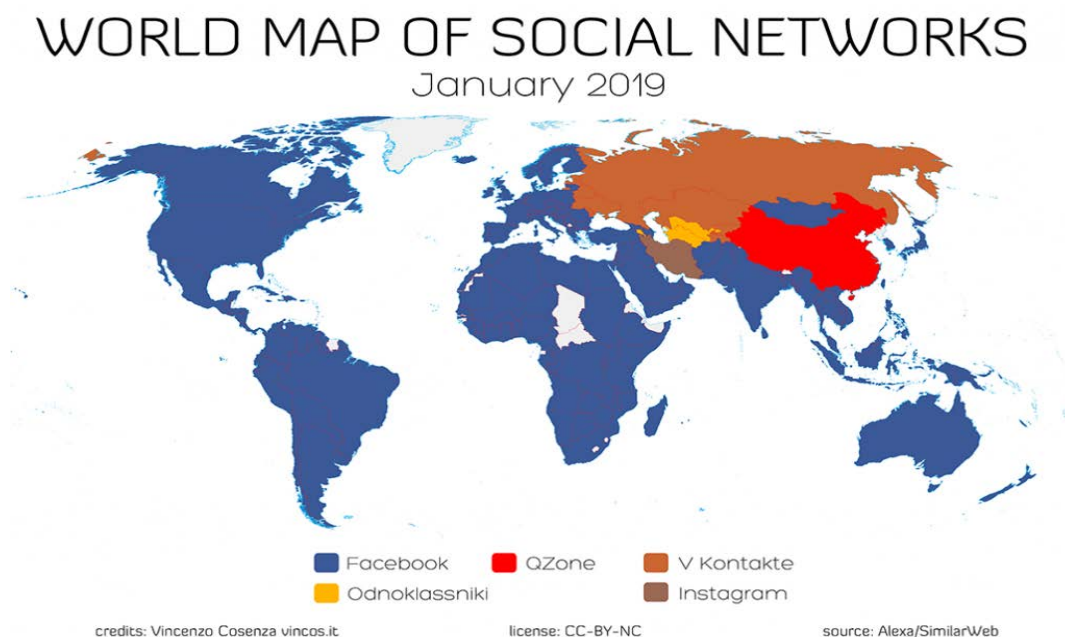
1 paveikslas. Socialinių tinklų profilio turinys ir galimos vartotojo pasirinktys

Šaltinis: sudaryta remiantis: Dovilės Prielaidienės magistro darbu „STS profilio turinys ir galimos vartotojo pasirinktys“ 2011.

²¹ JURKEVIČIENĖ, Jurgita. *Elektroniniai socialiniai tinklai naujosiose socialinėse medijose: dalyviai ir jų veiklos*: daktaro disertacija. Socialiniai mokslai, sociologija (05S) p.17-18.

Socialinių tinklų veikimo principą bei panaudojimo galimybes pavaizduoja 1 pav. Visų pirma pats vartotojas savo laisva valia susikuria taip vadinamą asmeninį profilį, kuriame prašoma pateikti savo asmeninius duomenis: vardą, pavardę, adresą, gimimo datą, gyvenamosios vietos adresą bei prašoma sutikti su visomis socialinio tinklo sąlygomis. Susikūręs profilį vartotojas gali dalintis nuotraukomis ant savo „sienos angl.-feed“ , naujienomis, kelti diskusijas, kviesti draugauti kitus arba sekti įdomius puslapius (angl. follow), gali viešinti arba nustatyti tam tikrą asmenų ratą, kas gali matyti jo skelbimus (angl.post), taip pat gali komentuoti kitų vartotojų viešus skelbimus, dalintis, pažymėti kitus savo draugus, reikšti nuomonę, siųsti individualią žinutę – bendrauti su kitais. Galbūt toks aiškus ir paprastas pateikimas išmaniuosiuose įrenginiuose bei naudojimąs automatizuotomis priemonėmis pritaikia vis daugiau vartotojų. Interneto vartotojų skaičius pasaulyje jau viršijo 4 milijardus vartotojų, taigi daugiau nei 55 % visos žmonijos populiacijos naudojami internetu ryšiu (Internet World Stats, 2018).²²

Visame pasaulyje šiuo metu populiariausias socialinis tinklas – „Facebook“. Drąsiai galima teigti, kad juo naudojasi daugiau nei pusė pasaulio valstybių (žr.į pav.2).



2 paveikslas. Socialinių tinklų žemėlapis 2019

Šaltinis: Sudaryta remiantis: Vincos pateikiama statistika apie socialinius tinklus. Prieiga per internetą: <<https://vincos.it/world-map-of-social-networks/>>.

²² SABAITYTĖ, J.; KARPORAVIČIŪTĖ, R. Didžiųjų duomenų panaudojimas socialinėje medijoje. *Mokslas – Lietuvos ateitis*, 2019, p.1–13.

Socialinių tinklų populiarumą lemia vis sparčiau tobulėjanti elektroninė erdvė, todėl socialiniai tinklai šiandieniniame pasaulyje atlieka ne tik bendravimo funkciją. Šiandien socialinių tinklų pasekmė yra tiesioginė rinkodara, kurios tikslu renkami asmens duomenys ir taip greičiau parduodamos prekės bei siūlomos paslaugos taip pat kitos pasekmės, kurios detaliau aptariamos sekančiame skyriuje.

1.3 Socialinių tinklų teigiamos ir neigiamos pasekmės

Socialinių tinklų sąvoka kaip jau buvo minėta yra kintanti. Šiandien socialiniai tinklai yra pakitę vertinant su pirmaisiais atsiradusiais. Jų sąvoka apima ne tik bendravimo pradinę funkciją. Tobulėjant technologijoms, tobulėja ir socialinių tinklų teikiamų paslaugų ratas. Remiantis užsienio autorių apibrėžimais apie socialines medijas, galima išskirti teigiamą įtaką bei naudą darančias socialinių tinklų pasekmes (žr. į 1 lentelę), ir neigiamas.

Visuomenės informavimo priemonė – ne paslaptis, kad socialiniuose šiuo metu daug informacijos, viena iš rūšių – skelbiama žiniasklaidos. Kaip anksčiau buvo minėta, socialiniais tinklais naudojasi vis daugiau asmenų, todėl socialiniuose tinkluose skelbiama visa aktualiusia visuomenei informacija: naujausios žinios, politinės aktualijos, kriminaliniai įvykiai, orų prognozės. Taip pat socialiniais tinklais neretai yra naudojama ir prašant pagalbos ieškant nusikaltusių ar dėl neaiškių aplinkybių dingusių žmonių. Taip pat socialiniai tinklai sukūrė remiantis Bozarth teigimu, kitokį informacinį turinį nei buvo įprasta skaityti rašytojų knygas, žurnalistų straipsnius, tai nauja, kuriama pačių vartotojų forma - tinklaraščiai, kuriuose dalinamasi įvairia informacija, dažniausiai ji susijusi su tinklaraštį kuriančio žmogaus asmenine patirtimi pvz.: vartotojas dalinasi apie keliones, kuriose buvo, aprašo, ką verta aplankyti, kur skaniai pavalgyti, ką nusipirkti. Tokio formato informacijos pateikimas sulaukia daug susidomėjimo ne tik iš vartotojų norinčių, sužinoti, ar verta keliauti būtent į tą vietą, pirkti tuos daiktus, bet ir marketingo specialistų.

1 lentelė. Termino „naujosios socialinės medijos“ interpretacijų įvairovė

Definicijos	Autoriai
[Naujosios] socialinės medijos reiškia visuomenės kuriamą internetinį turinį, besiskiriantį nuo generuojamo profesionalų, rašytojų, žurnalistų, pramonininkų ar žiniasklaidos. Socialinių technologijų, naudojamų socialinių medijų kūrimui, pavyzdžiai apima skirtus komunikacijai (tokie kaip tinklaraščiai), bendradarbiavimui (tokie kaip viki), bendruomenėms (tokie kaip Facebook), apžvalgoms bei nuomonėms (tokie kaip Amazon skaitytojų apžvalgos) ir multimedijai (tokie kaip YouTube).	Bozarth (2010: 11)
Naujosios] socialinės medijos yra žmonių tarpusavio sąveika, kurios rezultatas – svarbi, sensinga informacija, naudojant interneto technologiją kaip svarbiausią komunikacijos kanalą	Brown (2008: 35)
[Naujosios] socialinės medijos yra visiems prieinamos internetinės medijos, kuriose naujienos, nuotraukos, vaizdo įrašai ir radijo laidos yra vieši, paprastai lydimi balsavimo proceso, objektų populiarumui žymėti.	Evans (2008: 46)
[Naujosios] socialinės medijos – tai platus terminas, apibūdinantis visas tinklines mobiliąsias paslaugas, kurios suteikia individams galimybę sudaryti asmeninius profilius,	Funk (2011: 8)

Tęsinys kitame puslapyje

susisiekti su kitais vartotojais ir kurti, skelbti, atsakyti į turinį, dalintis juo su tinklu draugų arba internetu apskritai.	
Terminas [naujosios] socialinės medijos yra apie dalyvavimą. Šis dalyvavimas gali įgyti svarbios informacijos, kuri anksčiau buvo neprieinama, apžvalgos pavidalą. Vis dėlto kur kas dažniau jis įgyja komunikavimo, bendradarbiavimo bei susisiekimo su bet kuo, bet kur ir bet kuriuo metu, formą. Tai sietina su žmonių – asmenų ir grupių – sąveika ir dideliu potencialu daugiau dalintis, sužinoti, nuveikti, nei mūsų seneliai galėjo kada nors įsivaizduoti esant įmanomą.	Jue ir kt. (2010: 4-5)
[Naujosios] socialinės medijos yra internetu pagrįstų taikomųjų programų grupė, sukurta ideologiniu bei technologiniu Web2 pagrindu, kuri leidžia kurti ir keistis vartotojų sugeneruotu turiniu.	Kaplan ir kt. (2010: 59)
[Naujosios] socialinės medijos – tai bet kokios dvikryptės komunikacijos priemonės ar būdai, apimantys vieną iš didžiulės naujųjų, paprastai internetu pagrįstų, technologijų įvairovės.	Levinson ir kt. (2010: 239)
[Naujosios] socialinės medijos yra būtent tai, ką nurodo pavadinimas: medijos, kurios yra socialinės. Vyksmas virtualioje socialinėje erdvėje, atspindi vyksmą realioje. Žmonės sąveikauja, diskutuoja, dalinasi interesais, įgyja pasitikėjimą bei pagarbą ir priima sprendimus – visa atlieka tą pačią akimirką arba realiu laiku.	Macy ir kt. (2010: 58)
[Naujosios] socialinės medijos yra kategorija Web 2.0 priemonių, tokių kaip tinklaraščiai ir viki, kurių pagalba žmonės kuria ir skleidžia turinį. Socialinių medijų naudojimas dažnai yra vadinamas žinių demokratizacija, nes jos gali pakeisti žmones iš pasyvių turinio vartotojų, į aktyvius kūrėjus, kai jie rašo bei komentuoja kitų parašytas žinutes, dalinasi turiniu, skatindami kitus kurti naujas žinias	Meister ir kt. (2010: 265)
[Naujosios] socialinės medijos apima bet kurią iš daugybės internetinių priemonių, kurios leidžia žmonėms, turintiems panašius interesus dalintis informacija, mokytis iš kitų, formuoti socialinį tinklą	Wilson (2010: 1)

Šaltinis: Sudaryta remiantis: 2015 m. Jurgitos Jurkevičienės daktaro disertacija „Elektroniniai socialiniai tinklai naujosiose socialinėse medijose: dalyviai ir jų veiklos“.

Komunikacija– visais laikais buvo neišvengiama sociumo gyvavimo sąlyga. Be bendravimo tarp žmonių nebūtų visuomenės, o be jos valstybių. Bendraudami žmonės dalinasi savo mintimis, išgyvenimais, patirtimis, išreiškia nuomonę apie juos dominančius įvykius. Socialiniuose tinkluose sudarytos visos sąlygos paprastai, greitai išreikšti savo nuomonę pakomentuojant, pasidalinant informacija arba diskutuojant privačia žinute su asmeniu.

Marketingo funkcija- socialinių tinklų aplinka yra puiki vieta vykdyti rinkodarą, nes pagal tam tikrus tiesioginės rinkodarus būdus panaudojant asmens duomenis, galima sugeneruoti, ko vartotojams reikia ir ką jie labiausiai norėtų ir galėtų sau leisti įsigyti. Toks marketingas vadinamas elektroniniu- tai viena iš marketingo rūšių. Pagal M.Kiški²³ el. marketingas skirstomas į : elektroninė reklaminė komunikaciją (rinkodara e-paštu); paieškos rinkodarą (rinkodara siejama su interneto paieškos rezultatais); reklaminiai tinklapiai, laukai ir antraštės; rinkodara socialiniuose tinkluose; alternatyvi elektroninė rinkodara (pvz., virusinė rinkodara). Šiame darbe analizuojami socialiniai tinklai ir asmens duomenų apsauga juose, todėl toliau bus kalbama apie rinkodarą socialiniuose tinkluose, kiti atvejai išsamiai neanalizuotini. Rinkodara socialiniuose tinkluose pasižymi tuo „Pasak Y.

²³ KIŠKIS, Mindaugas. Socialiniai iššūkiai tiesioginei elektroninei rinkodarai. *Ekonomika ir vadyba*. 2009, p. 431.

K. Jin ir K. E. Sook (2004), prekės ženklo kūrimas socialiniuose tinkluose yra neatsiejamas nuo emocinės ženklo daros. Autoriai pateikia prekės ženklo socialiniuose tinkluose rinkodaros modelį, įvardydami jį 3C. 3C rinkodaros modelis apima tris emocinius prekės ženklo socialiniuose tinkluose elementus: personalizavimą, pritaikymą individualiems poreikiams (angl. customization), komunikaciją (angl. communication) ir prekės ženklo taikymo patirtį (angl. culture), kuri sukuriama sąveikaujant minėtiems dviems elementams (suasmeninimas, komunikacija). Anot Y. K. Jin ir K. E. Sook (2004), šis strategijos modelis per emocinę prizmę (ryšius su vartotojais) socialiniuose tinkluose kuria prekės ženklo žinomumą ir unikalų identitetą.²⁴ Personalizavimas – reiškia, kad informacija skiriama apie prekių ženklą tam tikrai vartotojų grupei, kuriai pagal grupės sukūrimo tikslą ji sukurta remiantis tam tikra sistema. Pavyzdžiui.: grupė „X“, kurioje jungiasi vartotojai besidomintys plaukų puoselėjimo procedūromis ir jų atstatymo gaminiais, tokioje grupėje galima teigti, kad aktualu būtų siūlomos tokios prekės kaip šampūnai, kondicionieriai, aliejai ir pan. Tokioje grupėje abejotina, ar domintų vartotojus teikiama informacija apie automobilius, jų detales, vartotojai kryptingai jungiasi tikėdamiesi surasti bei gauti naudingos informacijos apie plaukų priežiūrą, todėl prekės tokiu atveju personalizuojamos pagal dominantį dalyką – plaukų priežiūrą nagrinėtu atveju. Pritaikymas individualiems poreikiams iš pirmo žvilgsnio galima pamanyti, jog tai sinonimas žodžiui personalizavimas, tačiau taip nėra. Sąvoka pritaikymas individualiems poreikiams reiškia, kad informacija priklauso nuo paties vartotojo, o ne nuo sukurtos sistemos kaip personalizavimo atveju²⁵. Šias dvi sąvokas galima atskirti pagal tai, kas imasi iniciatyvos. Pavyzdžiui.: asmuo renkasi tam tikrame „y“ batų tinklapyje sau batus, kurių dydis turėtų būti 38, juodos spalvos ir odiniai. Tai jis daro savo iniciatyva, o analizuotu prieš tai atveju dėl plaukų priežiūros, grupėje keliama informacija kitų asmenų ir ji prieinama, pats vartotojas neieško, o naudojami informacija nustatyta pagal sistemą. Personalizavimas apima individualizuotą turinį, struktūrą ir pateikimą, o pritaikymas individualiems poreikiams

Prie neigiamų pasekmių galima priskirti BDAR numatytų teisių pažeidimus - tai neteisėtas duomenų tvarkymas, kuomet duomenys yra tvarkomi be duomenų subjekto sutikimo, neinformavimas apie duomenų panaudojimą kokiam nors tikslui, pavyzdžiui, dėl

²⁴ JEZUKEVIČIŪTĖ, J.; DAVIDAVIČIENĖ, V. Prekės ženklo rinkodaros modelis socialiniuose tinkluose. *Mokslas – Lietuvos ateitis*, 2014, p.122.

²⁵ HSIEH, C.; CHEN, S. *A Cognitive Style Perspective to Handheld Devices: Customization vs. Personalization* [interaktyvus, žiūrėta 2019 m. rugsėjo 2 d.]. Prieiga per internetą: <<https://files.eric.ed.gov/fulltext/EJ1090869.pdf>>.

minėtos tiesioginės rinkodaros, kaip toliau darbe bus nagrinėjama, asmens duomenys yra perduodami trečiosioms šalims be duomenų subjekto informavimo ir sutikimo. Norint, aiškiau suprasti, kokios yra neigiamos socialinių tinklų pasekmės, svarbu paanalizuoti BDAR ir jo taikymą iš kurio galima bus suprasti, su kokiais pavojais susiduria socialinių tinklų vartotojai – duomenų subjektai ir kaip turi būti užtikrinama duomenų apsauga taikant BDAR.

2.BDAR ASMENS DUOMENŲ APSAUGOS TAIKYMO RIBOS SOCIALINIAMS TINKLAMS

2.1 Asmens duomenų sąvokos analizė

Ši sąvoka įtvirtina BDAR 4 str. 1) „Asmens duomenys – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas); fizinis asmuo, kurio tapatybę galima nustatyti, yra asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius.“ Tačiau ši sąvoka nėra pakankamai aiškiai, tiksliai, išsamiai reglamentuota, todėl vertėtų išanalizuoti detaliau.

Išskirtini keturi esminiai požymiai apibūdinantys asmens duomenų sąvoką - asmens duomenys - bet kuri informacija; ji yra susijusi²⁶; su fiziniu asmeniu; kurio tapatybę gali būti nustatyta.²⁷ Šiuos požymius detalizuoja ES 29 str. darbo grupės nuomonė dėl asmens duomenų sąvokos²⁸. „Bet kuri informacija“ – tai absoliučiai visa įmanoma informacija apie asmenį: vardas, pavardė, asmens kodas, gyvenamosios vietos adresas, informacija apie privatų gyvenimą, darbo santykius, sveikatą, plaukų spalvą, genetinius ir biometrinius duomenis: pirštų atspaudai, rainelės struktūra, veido struktūra, balsas, rankos geometrija. Taip pat tai gali būti tiek objektyvi - duomenys apie sveikatos sutrikimus, kurie įrašyti į paciento ligos istoriją, tiek subjektyvi – darbdavio rekomendacija apie darbuotoją ir t.t. Pabrėžtina, kad asmens duomenimis laikoma informacija neturi būti teisinga, ar įrodyta. Tai reiškia, kad yra numatytos teisinės priemonės neteisingai informacijai užginčyti leidus duomenų subjektui susipažinti su informacija, todėl poreikio *a priori* įrodinėti kiekvieną asmens duomenį nebūtų tikslinga. „Bet kokiai informacijai“ informacijai pateikti nėra keliami formato reikalavimai, tai gali būti tiek rašytinis tekstas, tiek nuotraukos, skaičiai, garso įrašas, filmuota medžiaga. Taip informacijos užfiksavimo laikmenai nėra numatyti imperatyvūs reikalavimai, tai gali būti USB, DVD, CD formatu ir t.t. Asmens duomenų paviešinimas nepanaikina teisinės apsaugos. Tai aktualu socialiniuose tinkluose

²⁶ 1980 m. Ekonominio bendradarbiavimo ir plėtros organizacijos privatumo gairės [interaktyvus, žiūrėta 2019 m. rugsėjo 15 d.]. Prieiga per internetą: <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

²⁷ 1981 m. sausio 28 d. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) pakeista 2018 m. gegužės 18d. protokolu (CETS Nr. 223) [interaktyvus, žiūrėta 2019 m. rugsėjo 24 d.]. Prieiga per internetą: <https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872>.

²⁸ ES 29 str. darbo grupės 2007 m. birželio 20 d. Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf.

„Facebook“ ir „Instagram“, kur vartotojai dalinasi savo asmenine informacija, ką jie veikia, ką valgo, kur keliauja, tačiau tai nereiškia, jog jų pasidalinta informacija galima naudoti savais kiekvienas tikslais. Taip užtikrina teisė į privatumą, apie kurios santykį nagrinėsime kitame skyriuje.

Tęsiant asmens duomenų sąvokos analizę vertintinas požymis informacijos, kuri „susijusi“. Informacija turi būti susieta su konkrečiu asmeniu. Sąsajumo ryšys gali pasireikšti tiek tiesiogiai, tiek netiesiogiai. Tiesioginės informacijos atveju pvz.: nuolaidų kortelėje nurodytas gyvenamosios vietos adresas. Iš to galima akivaizdžiai suvokti, kad tai asmens duomenys, nurodantys jo konkrečią gyvenamąją vietą. Netiesioginės informacijos atveju duomenys apie asmenį iš pradžių siejami su objektu, o po tik su konkrečiu asmeniu. Pvz.: namo vertė – objektas, kurio informacija nėra laikoma asmens duomenimis, tačiau esant specifinėms situacijoms, tai gali tapti asmens duomenimis, jei nekilnojamojo turto vertė bus vertinama dėl savininko mokesčių mokumo. Toks ryšys įvardinamas tiksliau kaip informacijos sąsaja per objektą. Sąsajumo požymis asmens duomenų teisės kontekste vertinamas tik, jei informacija susijusi su fiziniu asmeniu. BDAR preambulės 14 p. numato „šiuo reglamentu užtikrinama apsauga turėtų būti taikoma fiziniams asmenims tvarkant jų asmens duomenis, neatsižvelgiant į jų pilietybę ar gyvenamąją vietą. Šis reglamentas neapimama juridinių asmenų ir visų pirma su juridinio asmens statusą turinčių įmonių duomenų, įskaitant juridinio asmens pavadinimą, teisinę formą ir kontaktinius duomenis, tvarkymo.“ Juridiniai asmenys yra saugomi ne pagal BDAR, o pagal LR elektroninių ryšių įstatymą. Taip pat BDAR netaikomas mirusiems asmenims pagal preambulės 27 p. Tačiau minėta ES 29 str. darbo grupės nuomonėje 4/2007 dėl asmens duomenų sąvokos Nr. WP136 (2007) ²⁹įtvirtinti trys atvejai, kai mirusio asmens duomenys gali būti laikomi asmens duomenimis: „Viena vertus, duomenų valdytojas gali neturėti galimybės sužinoti, ar asmuo, su kuriuo duomenys yra susiję, gyvas ar miręs. Net jei jis gali tai padaryti, informacija apie mirusiuosius gali būti tvarkoma tokia pačia tvarka kaip ir informacija apie gyvuosius. Antra vertus, informacija apie mirusius asmenis taip pat gali būti susijusi su gyvais asmenimis. Pavyzdžiui, informacija, kad mirusioji Gaja sirgo hemofilija, rodo, jog jos sūnus Titas taip pat serga šia liga, nes ji susijusi su X chromosomoje esančiu genu. Todėl jei galima laikyti, kad informacija, kurią sudaro mirusio asmens duomenys, susijusi su gyvais asmenimis ir tai yra asmens duomenys, kuriems taikoma direktyva, mirusio asmens duomenims gali būti netiesiogiai taikoma duomenų apsaugos taisyklėmis teikiama apsauga. Trečia, informacijai apie mirusius asmenis gali būti taikoma speciali apsauga,

²⁹ *Ibid.*

kurią užtikrina taisyklių rinkiniai, nustatyti ne duomenų apsaugos teisės aktuose, nustatant tai, kas vadinama personalitas praeterita. Medicinos personalo pareiga saugoti slaptumą neišnyksta pacientui mirus. Nacionaliniais teisės aktais, reglamentuojančiais asmens teisę į savo atvaizdą ir garbę, apsauga gali būti suteikta ir mirusio asmens atminimui. Tačiau Nacionalinės teisės aktų leidėjai gali nuspręsti išplėsti nacionalinių duomenų apsaugos teisės aktų nuostatų taikymo sritį tiek, kad ji apimtų kai kuriuos su mirusių asmenų duomenų tvarkymu susijusius aspektus, jeigu to reikia teisėtam interesui.“ Taigi, mirusio asmens sąvoka asmens duomenų teisėje nėra subasoliutinama ir duomenys gali patekti į asmens duomenų teisės taikymo sritį, todėl kiekvienu atveju reiktų vertinti žinojimą apie mirties faktą, sąsajumą su konkrečiu fiziniu asmeniu bei teisinę pareigą dėl duomenų saugojimo.

Kita asmens duomenų sąvokos sąlyga susijusi su galėjimu nustatyti asmens tapatybę. Nustatyti asmens tapatybę tiesiogiai galima tik pagal vardą ir pavardę, o netiesiogiai žinant asmens kodą, telefono numerį, gyvenamosios vietos adresą, dinaminis IP adresą ir t.t bei pagal tam tikrą duomenų rinkinį – pagal BDAR 30 p. „, fiziniai asmenys gali būti susieti su savo įrenginių, taikomųjų programų, priemonių ir protokolų interneto identifikatoriais, pavyzdžiui, IP adresais, slapukų identifikatoriais, arba kitais identifikatoriais, pavyzdžiui, radijo dažninio atpažinimo žymenimis. Taip gali likti pėdsakų, kurie visų pirma kartu su unikaliais identifikatoriais ir kita serverių gauta informacija gali būti panaudoti fizinių asmenų profiliams kurti ir jiems identifikuoti.“ Dinaminiai IP adresai laikomi asmens duomenimis, jei tam tikrų institucijų pagalba arba tos srities profesionalų žiniomis galima indentifikuoti asmenį. Taip pat remiantis BDAR preambulės 26 p. nurodyti pseudoniminiai duomenys, kuriais yra paslepiama tapatybė. Tokios procedūros tikslas – sudaryti galimybę rinkti papildomus duomenis, susijusius su tuo pačiu asmeniu, kai jo tapatybės nustatyti nebūtina. Tai ypač aktualu mokslinių tyrimų ir statistikos sritims. Pseudonimą galima sukurti taip, kad jį būtų galima atsekti pagal tapatybės atitikimo sąrašus ir jų pseudonimus arba naudojantis dvikrypčiais šifravimo algoritmais pseudonimams kurti. Tapatybę paslėpti galima ir kitu būdu, kai tapatybės iš naujo nustatyti nebeįmanoma, pavyzdžiui, vienakrypčio šifravimo būdu, kuriuo paprastai sukuriami anonimiški duomenys. Šios procedūros veiksmingumas priklauso nuo sudėtingumo užšifravimo, kiek jis yra apsaugotas nuo pačio atsekimo, galimybės susieti su konkrečiu asmens veiksmu ir įrašais ir pan. Koduoti duomenys - klasikinis pseudonimo sukūrimo pavyzdys. Informacija būna susijusi su kodu pažymėtais asmenimis, o kodo raktas, susiejantis kodą su bendraisiais asmenų žymenimis tapatybei nustatyti (pavyzdžiui, vardu, pavarde, gimimo data, adresu), laikomas atskirai. Pvz.: neapibendrinti statistikos duomenys – statistikos departamentas

tam tikrą asmenį užkoduoja kodu iš skaičių ir/ar raidžių, kurį saugo kodų rakte, tačiau savaime tokia koduotė nepatenka į asmens duomenų teisės taikymo sritį, bet nusprendęs pasinaudoti tais duomenis, gali būti taikomi asmens duomenų tasyklės, jei yra galimybė tiesiogiai ar netiesiogiai nustatyti fizinių asmenų tapatybes. Duomenų apsaugos teisės principai netaikomi anoniminiams duomenims, kuriuos galima apibrėžti kaip bet kokią informaciją, susijusią su fiziniu asmeniu, kai asmens tapatybės negali nustatyti nei duomenų valdytojas, nei bet koks kitas asmuo, atsižvelgiant į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo asmens tapatybei nustatyti. „Anoniminiai tapę duomenys“ yra anoniminiai duomenys, anksčiau nurodę asmenį, kurio tapatybę buvo galima nustatyti, tačiau dabar to padaryti neįmanoma. Pvz.: statistiniai duomenys ir padrikos informacijos sujungimas - statistikai ne tikrai privalo laikytis duomenų apsaugos taisyklių, kad būtų užtikrintas statistinių tyrimų anonimiškumas, jiems dar nustatyta ypatinga pareiga saugoti profesinę paslaptį ir draudžiama viešai skelbti duomenis, kurie nėra anoniminiai. Keliama tesinė pareiga kiekvienu konkrečiu atveju nustatyti ribą, nuo kurios bus laikoma, kad galima nustatyti susijusių asmenų tapatybę. Jei miestelyje yra vienas gydytojas-stomatologas, o kiti 7000 gyventojai, tai bendrinis žodis gydytojas tampa nebeanonimiškas, nes galima lengvai suprasti ar nustatyti pasitelkus priemones, todėl toks anonimiškumas nėra teisėtas, o išreiškiantis diskriminaciją. Tokiu atveju ją reiktų pašalinti arba sumažinti tam tikromis priemonėmis atpažinimo galimybę.

Socialiniuose tinkluose asmenys norėdami tapti socialinio tinklo vartotojais, turi susikurti profilį pagal nagrinėtą anksčiau socialinių tinklų koncepciją. Susikurdami asmeninį profilį pvz.: „Facebook“³⁰, privalo pateikti vardą, pavardę, telefono numerį, gimimo datą, lytį. Šie duomenys atitinka pagal BDAR 4 str. 1) asmens duomenų apibrėžtį, kurią sudaro 4 būtini kriterijai. Pateikta „bet kuri informacija“ – vardas, pavardė, telefono numeris, lytis, gimimo data. „Susijusi“ informacija – ši informacija yra apie socialinio tinklo konkretų vartotoją ir ji susijusi tiesiogiai – sužinome apie asmenį iš registracijoje pateikiamo vardo ir pavardės. Informacija susijusi su „fiziniu asmeniu“ – socialiniuose tinkluose asmens duomenų apsauga bus taikoma tik fiziniams asmenims. „Tapatybę nustatyti“ – šiuo atveju galima tiesiogiai iš vardo ir pavardės. Svarbu pabrėžti, kad ankstesniame skyriuje įvertinta, kad iš esmės socialiniai tinklai šiandieniniame technologijų amžiuje yra ne tik bendravimo platforma, bet ir apibūdinami plačiau kaip asmens duomenų tvarkymu grindžiamas verslo modelis ir patenka į BDAR taikymo apimtį. Verslo modelį galima įrodyti per vykdomą tiesioginę rinkodarą socialiniuose tinkluose, kur

³⁰ „Facebook“ socialinio tinklo registracija [interaktyvus, žiūrėta 2019 m. lapkričio 18 d.]. Prieiga per internetą: < <https://www.facebook.com/> >.

renkama informacija susijusi su vartotojais, pavyzdžiui.: „Facebook“ socialinio tinklo duomenų politikoje³¹ nurodoma, kad duomenys tvarkomi: „Reklamuotojams teikiame ataskaitas apie tai, kokie žmonės mato jų reklamas, ir apie šių reklamų veiksmingumą,, ir „eikiame apibendrintus statistinius duomenis ir išvalgas, padedančius žmonėms ir įmonėms suprasti, kaip žmonės sąveikauja su jų įrašais, skelbimais, puslapiais, vaizdo įrašais ir kitu turiniu „Facebook“ produktuose ir kitur.“, „renkame informaciją iš kompiuterių, telefonų, prijungtų televizorių ir kitų prie interneto prijungtų jūsų naudojamų įrenginių, kurie gali būti susieti su mūsų Produktais, bei informaciją apie šiuos įrenginius, ir sujungiame šią informaciją jums naudojantis skirtingais įrenginiais. Pavyzdžiui, surinktą informaciją apie tai, kaip naudojate mūsų Produktus telefone, naudojame, kad galėtume geriau asmeniškai pritaikyti turinį (įskaitant reklamas) ar funkcijas, „Reklamuotojai, programėlių kūrėjai ir leidėjai gali mums siųsti informaciją per naudojamas „Facebook“ technologijas, įskaitant socialinius papildinius (pavyzdžiui, mygtuką „Patinka“). Šie partneriai teikia informacijos apie jūsų veiklą už „Facebook“ ribų, įskaitant informaciją apie įrenginį, lankomas svetaines, įsigytus pirkinius, matomas reklamas bei informaciją apie tai, kaip naudojate mūsų paslaugomis. Renkame turinį, pranešimus ir kitą informaciją, kurią teikiate naudodami mūsų Produktus, įskaitant informaciją, kurią teikiate registruodami paskyrą, kurdami ar bendrindami turinį, ir susirašinėdami ar bendraudami su kitais. Tai gali būti ir informacija, esanti jūsų pateikto turinio (pavyzdžiui, metaduomenų) viduje ar informacija apie šį turinį, pavyzdžiui, nuotraukos vieta ar failo sukūrimo data. Šiai informacijai gali būti priskiriama ir tai, ką matote naudodamiesi mūsų teikiamomis funkcijomis“. Apžvelgus kelis pavyzdžius „Facebook“ duomenų politikos dėl duomenų tvarkymo, matome, kad naudojama bet kuri informacija susijusi su fiziniu asmeniu informacija tiesioginei rinkodarai vykdyti: tiek socialinio tinklo paskyros, tiek naudojamų įrenginių kaip telefono, kompiuterių, lankomų svetainių ir perkamų prekių jose, taip pat informacija iš „Facebooko produktų“ - „Messengeris, Instagram“ platformos.

Taigi, išanalizavus asmens duomenų sąvoką, galima teigti, jog asmens duomenų sąvoka yra labai ir apimanti didelį kiekį informacijos, kuria gali būti ne tik asmens vardas, pavardė, telefono numeris bet ir socialiniuose tinkluose skelbiama informacija, susirašinėjimai, įrenginio informacija: kompiuteryje ar telefone esanti, elektroninėse svetainėse perkami produktai ir pan, ši informacija renkama ne bereikalo, tiesioginei rinkodarai vykdyti, todėl BDAR tikslas užtikrinanti asmens duomenų apsaugą socialiniuose tinkluose naudojant tokius duomenis. Už duomenų tvarkymą ir valdymą atsakingi paskirti

³¹ „Facebook“ duomenų politika [interaktyvus, žiūrėta 2019 m. lapkričio 18 d.]. Prieiga per internetą: <<https://lt-lt.facebook.com/privacy/explanation>>.

subjektai – duomenų valdytojas ir duomenų tvarkytojas, bet dažnai šie subjektai yra sutapatinami, todėl toliau bus nagrinėjamos šios sąvokos socialinių tinklų kontekste.

2.2 Asmens duomenų apsaugos valdytojas ir tvarkytojas socialiniuose tinkluose

Duomenų valdytojo ir tvarkytojo sąvokos reglamentuotos BDAR 4 str. Pastarojo straipsnio 7 p. nurodyta: „duomenų valdytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuris vienas ar drauge su kitais nustato duomenų tvarkymo tikslus ir priemones; kai tokio duomenų tvarkymo tikslai ir priemonės nustatyti Sąjungos arba valstybės narės teisės, duomenų valdytojas arba konkretūs jo skyrimo kriterijai gali būti nustatyti Sąjungos arba valstybės narės teise“, o 8 p. „duomenų tvarkytojas – fizinis arba juridinis asmuo, valdžios institucija, agentūra ar kita įstaiga, kuri duomenų valdytojo vardu tvarko asmens duomenis.“ Lingvistiškai požiūriu vertinant duomenų valdytojas nuo duomenų tvarkytojo skiriasi tuo, kad duomenų tvarkytojas tvarko asmens duomenis duomenų tvarkytojui liepus ir visa atsakomybė dėl asmens duomenų tenk duomenų valdytojui. Šios sąvokos išsamiau paaiškintos ES 29 str. darbo grupės 2010 m. vasario 16 d. nuomonėje Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“. ³²Pažymėtina, kad ES darbo grupės 29 str. nuomonė buvo parengta pagal 95/46 direktyvą, kurią panaikino BDAR, bet nuorodos į panaikintą direktyvą laikomos nuorodomis į šį reglamentą. Nuorodos į Direktyvos 95/46/EB 29 straipsniu įsteigtą Darbo grupę asmenų apsaugai tvarkant asmens duomenis laikomos nuorodomis į šiuo reglamentu įsteigtą Europos duomenų apsaugos valdybą³³. Vadinasi nuostatos duomenų valdytojo ir tvarkytojo atžvilgiu liko galioti tos pačios, todėl ši nuomonė aktuali. Sąvokos „duomenų valdytojas“ ir jos ryšys su sąvoka „duomenų tvarkytojas“ yra itin svarbūs taikant BDAR, nes nuo to priklauso, kas yra atsakingas už duomenų apsaugos taisyklių laikymąsi, kaip duomenų subjektai gali naudotis savo teisėmis, kokia nacionalinė teisė taikytina ir kaip veiksmingai gali dirbti duomenų apsaugos institucijos.

Duomenų valdytojams nustatytos pareigos pasireiškia per duomenų tvarkymą - pagal BDAR įtvirtinta teisinė prievolė duomenų subjektui gauti informaciją, leisti susipažinti su duomenimis, juos ištaisyti arba ištrinti, blokuoti arba prieštarauti duomenų tvarkymui.

³² 2010 m. vasario 16 d. ES 29 str. darbo grupės nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP169 [interaktyvus. žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.

³³ 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 2016 L 119, p. [interaktyvus, žiūrėta 2019 m. rugsėjo 22 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016R0679&from=lt>>.

Duomenų valdytojas privalo pagal sutartinius įsipareigojimus sudaryti visas galimybes ir būdus tokioms teisės įgyvendinti bei apdoroti duomenis saugiai ir teisėtai. Taip pat duomenų valdytojas atsakingas iš esmės už bet kokią dėl neteisėto duomenų tvarkymo padarytą žalą. Duomenų valdytojo sąvoka suprantama ir aiškinama plačiai. Juo gali būti tiek fizinis ar juridinis asmuo, valstybės valdžios institucija, agentūra ar bet kurį kitas organas, kuris vienas ar drauge su kitais nustato asmens duomenų tvarkymo tikslus ir būdus. ES Teisingumo Teismas jau yra nusprendęs, šios nuostatos tikslas – plačiai apibrėžti sąvoką „valdytojas“, kad būtų užtikrinta veiksminga ir visapusiška duomenų subjektų apsauga.³⁴ Direktyvos 95/46 (dabar galiojantis BDAR) 2 straipsnio d punkte, sąvoka „duomenų valdytojas“ apima subjektą, kuris „vienas ar drauge su kitais“ nustato asmens duomenų tvarkymo tikslus ir būdus, ši sąvoka nebūtinai reiškia vieną subjektą ir gali apimti kelis dalyvius tvarkant šiuos duomenis, kurių kiekvienam atitinkamai galioja duomenų apsaugai taikomos teisės normos.³⁵ Šiame teiginyje paminėtini BDAR 26 str. 1d., 2d., 3d., kuris numato, kad duomenų valdytojai gali būti bendri, kai du ar daugiau nustato duomenų tvarkymo tikslus bei priemones. Atsakomybę bendri valdytojai laisvu ir skaidriu susitarimu patys nusistato tarpusavyje, tačiau duomenų subjektas gali naudotis savo teisėmis pagal BDAR kiekvieno iš duomenų valdytojų atžvilgiu.

Socialinių tinklų teikėjai yra duomenų valdytojai pagal BDAR. Jie suteikia priemones vartotojo duomenims apdoroti ir teikia visas „pagrindines“ paslaugas, susijusias su vartotojo valdymu (pvz., Paskyrų registravimą ir ištrynimą). Socialinių tinklų teikėjai taip pat nustato, kaip naudotojų duomenys gali būti naudojami reklamos ir rinkodaros tikslams, įskaitant trečiųjų šalių teikiamą reklamą.³⁶ Socialiniuose tinkluose „Facebook“ ir „Instagram“ duomenų valdytojas yra bendrovė „Facebook Ireland“. Šių socialinių tinklų duomenų valdytojas renka paprastai ir trumpai tariant „visą“ informaciją t.y. pradedant nuo užsiregistravimo: vardo, pavardės, gimimo datos, lyties ir baigiant privačiais susirašinėjimais, nuotraukų padarymo vietomis bei net su koku fotoaparatu padarytomis. Renkama informacija apie žmones, puslapius, paskyras, saitazodžius ir grupes, prie kurių vartotojai prisijungę, bei informaciją apie tai, kaip su jais sąveikaujama naudojant Facebook/Instagram funkcijas, pavyzdžiui, su kokiais žmonėmis daugiausia bendraujama

³⁴ ES Teisingumo teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*, 34 p. [interaktyvus, žiūrėta 2019 m. spalio 1 d.]. Prieiga per internetą: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=LT>>.

³⁵ *Ibid.*

³⁶ 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

ar kokioms grupėms priklausoma.³⁷ Renkama kontaktinė, įrenginių informacija. Svarbu pabrėžti, kad tai nėra vieninteliai duomenų valdytojai šiuose socialiniuose tinkluose. 2018 m. asmens duomenų valdytojų sąvoka socialiniame tinkle „Facebook“ buvo išplėsta.³⁸ Ginčas kilo dėl Vokietijoje, „Facebook“ platformoje sukurtame „Gerbėjų puslapyje“, kuriame gerbėjų tinklalapio autorius, užsiregistravęs „Facebook“, gali naudoti šio tinklo sukurtą platformą, siekdamas prisistatyti šio socialinio tinklo vartotojams ir gerbėjų tinklalapyje apsilankiusiems asmenims, taip pat skelbti įvairaus pobūdžio pranešimus žiniasklaidos ir nuomonės formavimo rinkoje. Gerbėjų tinklalapių administratoriai gali gauti anoniminius statistinius duomenis apie šių tinklalapių lankytojus, naudodami įrankį „Facebook Insight“, kurį „Facebook“ jiems suteikia nemokamai naudotis nekeičiamomis sąlygomis. Šie duomenys renkami naudojant slapukus, kurių kiekvienas turi unikalų naudotojo kodą; jie veikia dvejus metus ir „Facebook“ juos išsaugo gerbėjų tinklalapyje apsilankiusio asmens kompiuterio standžiajame diske arba bet kurioje kitoje laikmenoje. Naudotojo numeris, kurį galima susieti su „Facebook“ prisiregistravusių vartotojų prisijungimo duomenimis, gaunamas ir tvarkomas atidarant gerbėjų tinklalapius. Šiuo klausimu iš prašymo priimti prejudicinį sprendimą matyti, kad nei „Wirtschaftsakademie“, nei „Facebook Ireland Ltd“ nepranešė apie slapukų išsaugojimo operaciją ir veikimą arba apie tolesnį duomenų tvarkymą, bent jau pagrindinėje byloje reikšmingu laikotarpiu.³⁹ Šioje byloje nustatyta, kad sukurdamas Facebook gerbėjų puslapį administratorius turėjo pareigą su „Facebook Ireland“ sudaryti specialią sutartį dėl tokio tinklalapio atidarymo ir dėl sutikimo su tokio tinklalapio naudojimo sąlygomis, įskaitant susijusią slapukų politiką. Nors „Facebook“ parengta auditorijos statistinė informacija perduodama gerbėjų tinklalapio administratoriui tik anonimine forma, vis dėlto naudojant slapukus, kuriuos „Facebook“ įdiegia šiame tinklalapyje apsilankiusio asmens kompiuteryje arba bet kuriame kitame įrenginyje, šiai statistikai parengti prieš tai yra renkami ir apdorojami šių lankytojų asmens duomenys. Bet kuriuo atveju Direktyvoje 95/46 (dabar galioja BDAR) nereikalaujama, kad solidarios kelių ūkio subjektų atsakomybės už tą patį duomenų tvarkymą atveju kiekvienas jų turėtų prieigą prie atitinkamų asmens duomenų. Tokiomis aplinkybėmis manytina, kad „Facebook“ esančio gerbėjų tinklalapio administratorius, kaip

³⁷ Duomenų politika [interaktyvus, žiūrėta 2019 m. spalio 16 d.]. Prieiga per internetą: <<https://lt.lt.facebook.com/help/instagram/155833707900388>>.

³⁸ Tarptautinis Teisingumo teismas. 2018 m. birželio 5 d. sprendimas *Vokietijos regioninė duomenų apsaugos institucija prieš Vokietijos mokymo bendrovę GmbH* [interaktyvus, žiūrėta 2019 m. rugsėjo 16 d.]. Prieiga per internetą:

<<http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=LT>>.

³⁹ *Ibid.*, 15 p.

antai „Wirtschaftsakademie“, 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 nagrinėjamu atveju jis kartu su „Facebook Ireland“ turi būti laikomas tokių duomenų valdytoju, kaip tai suprantama pagal Direktyvos 95/46 2 straipsnio d punktą. Taigi duomenų valdytoju socialiniuose tinkluose gali būti bet kas, kas naudojasi slapukais prieš tai sudarydamas sutartį dėl tokio tinklalapio ir taip renka asmens duomenis apie vartotojus.

Duomenų tvarkytojas (BDAR 4 str. 8 p., 28 str. ET duomenų apsaugos konvencijos 2 str. f p.) – tai subjektas, kurio teisinės pareigos priklauso nuo duomenų valdytojo sprendimo; duomenų valdytojas gali nuspręsti tvarkyti duomenis savo organizacijoje arba patikėti visą duomenų tvarkymo veiklą ar jos dalį išorės organizacijai. Duomenų tvarkytojas turi tenkinti dvi pagrindines sąlygas: pirma, jis turi būti duomenų valdytojo atžvilgiu savarankiškas juridinis asmuo; antra, jis turi tvarkyti asmens duomenis duomenų valdytojo vardu.⁴⁰ Duomenų tvarkytojas priešingai nei duomenų valdytojas atsako ribota apimti pagal BDAR. Teigiama, kad sąvokos duomenų valdytojas ir tvarkytojas buvo sugalvotos tam kad, išspręstų atsakomybės pasidalijimo klausimą. Tikslas tokio pasidalijimo – pagal teisinės pareigas numatytas BDAR, žinoti į ką kreiptis esant asmens duomenų apsaugos pažeidimams pvz.: duomenų panaudojimas ne pagal tikslą, perteklinių duomenų reikalavimai, duomenų naudojimas be subjekto informavimo ir pan. Tačiau toks atskyrimas viena vertus palengvino atsakomybės klausimą, bet kita vertus dažnai sunku nustatyti, kuris yra kuris, neretai teisės ir pareigos persipina ir duomenų tvarkytojui tai pat ten atsakyti už neteisėtus veiksmus. Kaip pavyzdį galima pateikti šią socialinio tinklo „Facebook“ situaciją: „Facebook“ reklamos atveju patvirtino, kad jūs mokate už skelbimą jų svetainėje, jie naudojami savo vartotojų duomenimis, kad nuspręstų, kam rodoma ta reklama, remiantis jūsų nustatytais parametrais. Jums nereikia tvarkyti asmenų duomenų - visa tai daro „Facebook“. Jūs esate mokantis klientas, kuris nėra nei duomenų valdytojas, nei duomenų tvarkytojas. „Facebook“ yra duomenų tvarkytojas. Kai įkeliate dabartinių klientų el. pašto adresų sąrašą, kad sukurtumėte pasirinktinę auditoriją, tada jūs tampate duomenų valdytoju, o „Facebook“ tampa duomenų tvarkytoju - jūs esate atsakingi už duomenų, kuriuos teikiate „Facebook“, vientisumą. „Facebook“ išlaiko pasirinktinių auditorijų funkciją, tačiau vėl įdeda prekės ženklo atsakomybę, kad įsitikintų, jog duomenys yra tinkami naudoti ir kad sutikimas buvo gautas.⁴¹ Tokiu atveju gali kilti

⁴⁰ 2010 m. vasario 16 d. ES 29 str. darbo grupės nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP169 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.

⁴¹ C/net tinklapis [interaktyvus, žiūrėta 2019 lapkričio 18 d.]. Prieiga per internetą:

klausimas, ar vartotojas naudodamasis duomenimis tampa duomenų valdytoju? Asmeninių poreikių išimtis numatyta BDAR 2 str. 2 d. c) p., kuris nurodo, kad BDAR nėra taikomas, kai duomenis tvarko fizinis asmuo, užsiimdamas išimtinai asmenine ar namų ūkio veikla. Asmeninę ar namų ūkio priežiūros veiklą gali sudaryti, be kita ko, susirašinėjimas ir adresų saugojimas arba naudojimas socialiniais tinklais ir internetinė veikla, vykdoma atliekant tokią veiklą. Tačiau šis reglamentas taikomas duomenų valdytojams arba duomenų tvarkytojams, kurie suteikia priemones asmens duomenų tvarkymui vykdant tokią asmeninę ar namų ūkio priežiūros veiklą (BDAR preambulės 18 p.). BDAR netaikomas, jei socialinių tinklų vartotojas veikia įmonės ar asociacijos vardu, ar naudoja socialinius tinklus daugiausia kaip platforma komerciniams, politiniams ar labdaros tikslams pasiekti, taip pat socialiniai tinklai turėtų užtikrinti privatumą užtikrinančius ir nemokamus numatytuosius nustatymus, kurie riboja prieigą prie pačių pasirinktų kontaktų. Kai prieiga prie profilio informacijos apima ne tik jūsų pasirinktus kontaktus, pvz., kai prieiga prie profilio suteikiama visiems socialinių tinklų nariams arba duomenys yra indeksuojami paieškos sistemose, prieiga peržengia asmeninę ar namų ūkio sritį. Lygiai taip pat, jei vartotojas priima pagrįstą sprendimą išplėsti prieigą, neapsiribodamas savo paties pasirinktais „draugų“ duomenų valdytojo įsipareigojimais. Namų ūkio išimties taikymą taip pat riboja poreikis užtikrinti trečiųjų šalių teises, ypač dėl neskelbtinų duomenų. Be to, reikia pažymėti kad net jei taikoma namų ūkio išimtis, vartotojas gali būti atsakingas pagal atitinkamų nacionalinių civilinių ar baudžiamųjų įstatymų bendrąsias nuostatas (pvz., šmeižtas, baudžiamoji atsakomybė ir pan).⁴²

Taigi, išanalizavus duomenų tvarkytojo ir valdytojo sąvokas, galima teigti, kad atskyrimas ir santykis vieno su kitu yra būtinas asmens duomenų apsaugos atžvilgiu nustatant atsakomybę už BDAR pažeidimus. Jei socialinių tinklų vartotojas vykdo asmeninę veiklą savo poreikiams nesidalindamas ir neplatindamas duomenų komerciniais ar kitais tikslais ir neperžengia namų ūkio veiklos ribų, jis nelaikomas nei duomenų tvarkytoju, nei duomenų valdytoju kaip tai suprantama pagal BDAR. Socialiniuose tinkluose vartotojai pagal nagrinėtą socialinių tinklų koncepciją dažnai skelbia asmeninius duomenis ir neretai susiduriama su situacija: jei duomenys paskelbi, prieinami ir matomi kitiems vartotojams, reiškia juos galima tvarkyti savo tikslais, tačiau, ar tai teisėta iš tikrųjų

<<https://www.cnet.com/news/facebook-to-build-custom-audiences-tool-to-fight-advertising-without-consent/>>.

⁴² 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

pagal BDAR? Toliau bus analizuojamas asmens duomenų ir privatumo santykis socialiniuose tinkluose.

2.3 Privatumo santykis su asmens duomenimis virtualioje erdvėje

Privatumo sąvoka yra neatsiejama nuo socialinių tinklų, nes juose (kaip jau buvo ne kartą paminėta) kaupiami dideli duomenų kiekiai susiję su fiziniais asmenimis: duomenys apie vartotoją, jo gyvenamąją vietą, informacija apie darbovietę ar mokymosi įstaigą, kitus vartotojus su kuriais bendrauja, santykių ryšiai su artimais žmonėmis bei giminėmis, duomenys, kuriais dalinasi: nuotraukos, lokacijų žymėjimas, komentarai, mėgiamos grupės, naršomi kiti puslapiai ir t.t. Todėl iškyla klausimas, kur yra riba tarp teisės į privatumą ir asmens duomenų skelbimo socialinėje erdvėje? Ar kas paskelbta asmens, tampa automatiškai sutikimu naudoti duomenis kitiems subjektams savo tikslais?

Teisė į privatumą apima pačią jautriausią informaciją susijusią su fiziniu asmeniu t.y., privatų, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą be leidimo publikuoti asmenines nuotraukas, draudimą skelbti gautą ar surinktą konfidencialią informaciją.⁴³ Teisė į privatumą reguliuojama tiek tarptautiniu, tiek europiniu bei nacionaliniu lygiu. Privatumo teisė įtvirtinta Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijoje, kurios 8 straipsnio 1 dalyje numatyta, kad kiekvienas turi teisę į tai, jog būtų gerbiamas jo asmeninis ir jo šeimos gyvenimas, buto neliečiamybė ir susirašinėjimo slaptumas. Europos Žmogaus Teisių Teismas yra išaiškinęs, jog duomenų, susijusių su privačiu asmens gyvenimu, laikymas, taip pat ir jų panaudojimas patenka į Konvencijos 8 straipsnio veikimo sritį (žr., pvz., 2008 m. gruodžio 4 d. sprendimą S. ir Marper prieš Jungtinę Karalystę (pareiškimo Nr. 30566/04). Taip pat niekas neturi patirti savavališko kišimosi į jo privatumą, šeimos gyvenimą, buitį ar susirašinėjimą arba kėsಿನimosi į jo garbę ir reputaciją. Kiekvienas turi teisę į įstatymo apsaugą nuo tokio kišimosi arba kėsಿನimosi.⁴⁴ Europos Teisingumo Teismas toliau ESTT) savo praktikoje primena, jog Direktyvos 95/46/EB (dabar galiojantis BDAR) nuostatos, reglamentuojančios asmens duomenų tvarkymą, dėl kurio gali būti pažeistos pagrindinės laisvės, ypač teisė į privatų gyvenimą, turi būti būtinai aiškinamos atsižvelgiant į Chartijoje garantuojamas pagrindines teises (žr. 2003 m. gegužės 20 d. sprendimo Österreichischer Rundfunk ir kt., C-465/00, C-138/01 ir C-139/01, 68 punktą; 2014 m. gegužės 13 d. sprendimo Google Spain ir Google, C-131/12, 68 punktą, 2015 m.

⁴³ 1970 m. sausio 23 d. Europos Tarybos Parlamentinės Asamblėjos rezoliucija Nr. 428/1970 „Dėl masinės informacijos priemonių ir žmogaus teisių“. [interaktyvus, žiūrėta 2019 spalio 3d.]. Prieiga per internetą:<<http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en>>.

⁴⁴ 1948 m. gruodžio 10 d. Generalinės Asamblėjos Visuotinė žmogaus teisių deklaracija. *Valstybės žinios*, 2006, nr. 68-2497 16 str.

spalio 6 d. sprendimo Maximillian Schrems prieš Data Protection Commissioner, C-362/14, 38 punktą).

Lietuvoje teisė į privatumą įtvirtinta Konstitucijos 22 str. „Žmogaus privatus gyvenimas neliečiamas. Asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas neliečiami. Informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą. Įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinosi į jo garbę ir orumą.“ Ši teisė apima asmeninį, šeimos ir namų gyvenimą, asmens fizinę ir psichinę neliečiamybę, garbę ir reputaciją, asmeninių faktų slaptumą, draudimą skelbti gautą ar surinktą konfidencialią informaciją ir kt. Savavališkai ir neteisėtai kišantis į žmogaus privatų gyvenimą kartu yra kėsinamasi į jo garbę bei orumą.⁴⁵ Konstitucinis Teismas taip pat yra nurodęs, jog Konstitucijos 25 straipsnio 3 dalis, kurioje *inter alia* įtvirtinta, kad laisvė gauti informaciją gali būti ribojama įstatymu, jei tai būtina apsaugoti žmogaus privačiam gyvenimui, glaudžiai susijusi su Konstitucijos 22 straipsnio nuostatomis, kuriose įtvirtintas žmogaus privataus gyvenimo neliečiamumas.⁴⁶ Taip pat klausimai susiję su duomenimis reguliuojami ir LR Asmens duomenų teisinės apsaugos įstatymu, kurio pagrindu duomenys turi būti renkami teisėtais ir konkrečiai apibrėžtais tikslais, tvarkomai tiksliai ir sąžiningai bei teisėtais pagrindais, saugomi tiek laiko, kiek reikia tiems tikslams įgyvendinti taip įtvirtina privatumo imperatyvą imperatyvą. Trumpai tariant teisė į privatumą sudaro 4 dalys apimančios teisę į kūno neliečiamybę, komunikacijų, teritorinį bei informacinį (žr. į 2 lentelę).

2 lentelė. Privatumo sąvokos elementai

Privatumo sudėtinės dalys	
Kūno	Saugo asmens kūną nuo tokių invazinių procedūrų kaip narkotikų testai, kratos ir pan.
Komunikacijų	Saugo telefono, el.pašto ir kitas komunikacijas

Tęsinys kitame puslapyje

⁴⁵ Lietuvos Respublikos Konstitucinis teismas. 2000 m. gegužės 8 d. nutarimas dėl Lietuvos Respublikos operatyvinės veiklos įstatymo 2 straipsnio 12 dalies, 7 straipsnio 2 dalies 3 punkto, 11 straipsnio 1 dalies ir Lietuvos Respublikos baudžiamojo proceso kodekso 198¹ straipsnio 1 bei 2 dalių atitikimo Lietuvos Respublikos Konstitucijai, Nr. 12/99-27/99-29/99-1/2000-2/2000.

⁴⁶ Lietuvos Respublikos Konstitucinis teismas. 2011 m. Birželio 9 d. Nutarimas dėl Lietuvos Respublikos nekilnojamojo turto registro įstatymo (2001 m. Birželio 21 d. Redakcija) 42 straipsnio atitikties Lietuvos Respublikos Konstitucijai ir Lietuvos Respublikos vyriausybės 2002 m. Liepos 12 d. Nutarimu nr. 1129 „Dėl nekilnojamojo turto registro nuostatų patvirtinimo“ patvirtintų nekilnojamojo turto registro nuostatų 88 punkto (2007 m. Vasario 27 d. Redakcija), 97 punkto (2007 m. Vasario 27 d., 2008 m. Spalio 22 d., 2010 m. Kovo 3 d., 2011 m. Gegužės 4 d. Redakcijos) atitikties Lietuvos Respublikos Konstitucijai, Nr. 12/2008-45/2009.

Teritorinis	Saugo namų, darbo ir kitas aplinkas
Informacinis	Saugo informaciją apie asmenis, t.y. asmens duomenis

Šaltinis: Sudaryta remiantis: autorės pagal Juliaus Zaleskio monografiją „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“ 2019.

Vertinant asmens duomenų apsaugą, ją apimta tik asmens duomenys, kurie yra susiję su konkrečiu fiziniu asmeniu bei kurio tapatybė nustatyta arba galima ją nustatyti. Iš to galime daryti išvadą, kad teisė į privatumą yra platesnė sąvoka apimanti ir asmens duomenų apsaugą. Tai Europos Žmogaus Teisių Teismas (toliau – EŽTT) pripažįsta, kad teisė į privataus gyvenimo gerbimą tvarkant asmens duomenis siejama su visa informacija apie fizinį asmenį, kurio tapatybė nustatyta arba gali būti nustatyta (žr., be kita ko, EŽTT 2000 m. vasario 16 d. sprendimo byloje *Amann prieš Šveicariją*, peticijos Nr.28341/95, 65 punktą ir 2000 m. gegužės 4 d. sprendimo byloje *Rotaru prieš Rumuniją*, peticijos Nr. 28341/95, 43 punktą).

Socialiniuose tinkluose daugumai varotojų gali būti susidaręs toks įspūdis, jei asmuo pasidalina kažkia informacija susijusia su jo privačiu gyvenimu, tai ta informacija galima dalintis su kitais ypatingai toks mąstymas aktualus ir su viešais asmenimis, tačiau, ar tokie veiksmai iš tikrųjų yra teisėti? Ar pakanka to fakto, kad asmuo pasidalina asmenine informacija socialinėje platformoje ir tai jau reiškia, kad galima nepaprašius sutikimo dėl tokios asmeninės informacijos naudojimo, naudoti savo tikslais? Teisė į privatumą yra pasyvi asmens teisė, nes ją įgyvendina kiti subjektai, o ne pats asmuo aktyviai savo veiksmais.⁴⁷ Pagal EŽTT praktiką, Konvencijos 8 straipsniu valstybės ne tik įpareigojamos susilaikyti nuo bet kokių veiksmų, kuriais galėtų būti pažeidžiama ši Konvencijoje įtvirtinta teisė, bet ir tam tikromis aplinkybėmis joms taip pat taikomi pozityvūs įpareigojimai aktyviais veiksmais užtikrinti faktinę pagalbą privačiam ir šeimos gyvenimui (žr., pvz., 2008 m. liepos 17 d. sprendimą I. prieš Suomiją (pareiškimo Nr. 20511/03), 2008 m. gruodžio 2 d. sprendimą K. U. prieš Suomiją (pareiškimo Nr. 2872/02) EŽTT 2004 m. birželio 24 d. sprendime Von Hannover prieš Vokietiją dar kartą pažymėjo esminę privataus gyvenimo apsaugos svarbą kiekvieno žmogaus asmenybės raidos požiūriu ir konstatavo, kad ši apsauga apima ne tik privačią šeimos, bet ir socialinę erdvę, kad kiekvienas asmuo (net jei jis ir yra žinomas plačiajai visuomenei) turi turėti galimybę naudotis teise į teisėtą lūkestį dėl savo privataus gyvenimo apsaugos ir gerbimo. Įvertinus šią EŽTT teismų praktiką, galima teigti, kad nėra jokio skirtumo, ar viešas asmuo, ar ne –

⁴⁷ PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*. 2011, p. 166.

teisė į privatumą galioja tokia pačia apimti ir socialinėje erdvėje viešai skelbiant informacija apie save.

Socialiniuose tinkluose privatumo užtikrinimas numatytas vartotojų profilių nustatymuose. Duomenų valdytojai privalo imtis tinkamų techninių ir organizacinių priemonių „tiek tvarkymo sistemos projektavimo metu, tiek ir paties tvarkymo metu“, kad būtų išlaikytas saugumas ir užkirstas kelias neteisėtam tvarkymui, atsižvelgiant į duomenų tvarkymo ir duomenų tvarkymo keliamą riziką, duomenų pobūdį. Svarbus privatumo nustatymų elementas yra prieiga prie profilyje paskelbtų asmeninių duomenų. Jei tokiai prieigai nėra taikomi jokie apribojimai, trečiosios šalys gali susieti įvairius privačius duomenis apie vartotojus per socialinių tinklų narius arba per paieškos nuorodą. Tačiau tik mažuma vartotojų, prisiregistruojančių prie paslaugos, atliks bet kokius numatytųjų nustatymų pakeitimus. Todėl socialiniai tinklai turėtų siūlyti privatumą užtikrinančius numatytuosius nustatymus, kurie vartotojams leidžia laisvai ir konkrečiai sutikti su bet kuria prieiga prie savo profilio turinio siekiant sumažinti neteisėto tvarkymo iš trečiųjų šalių riziką.⁴⁸ *Sensitive data* liet. neskelbtini duomenys kitaip tariant privatus asmens duomenys laikomi: duomenys, atskleidžiantys rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose arba duomenys apie sveikatą ir lytinį gyvenimą. Privatus asmens duomenys gali būti skelbiami internete tik gavus aiškų duomenų subjekto sutikimą arba jei duomenų subjektas duomenis aiškiai paviešino pats. Kai kuriose ES valstybėse narėse duomenų subjektų atvaizdai laikomi specialia asmens duomenų kategorija, nes jie gali būti naudojami atskirti rasinę/etninę kilmę arba gali būti naudojami religiniams įsitikinimams ar sveikatos duomenims nustatyti. Paprastai ES 29 str. darbo grupė nemano, kad atvaizdai internete yra neskelbtini duomenys, nebent atvaizdai būtų aiškiai naudojami neskelbtiniems duomenims apie asmenis atskleisti.⁴⁹

Taigi teisė į privatumą yra ne BDAR sukurta nauja teisė, o jau seniai kiekvienam asmeniui garantuojama teisė nepaisant to, ar tai viešas asmuo, ar ne. Vertinant su asmens duomenų apsauga, privatumo teisė yra platesnė, apimanti ne tik asmens duomenų apsaugą, bet ir kūno, teritorinę, komunikacijų neliečiamybę. Socialiniuose tinkluose dėl skelbiamų jautrių duomenų apie asmenį kyla didelė rizika asmens privatumo teisei pažeisti, todėl duomenų valdytojai turi pareigą pasiulyti efektyviausias priemones vartotojams dėl prieigos prie tokių duomenų siekiant maksimaliai juos apsaugoti. Išanalizavus privatumo

⁴⁸ 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

⁴⁹ *Ibid.*

ir asmens duomenų apsaugos svarbą, toliau bus vertinami pagrindiniai BDAR numatyti reikalavimai duomenų valdytojams socialiniuose tinkluose.

3. SOCIALINIŲ TINKLŲ PAREIGOS ASMENS DUOMENŲ APSAUGAI UŽTIKRINTI

3.1 Teisėtumo, sąžiningumo ir skaidrumo principas asmens duomenų apsaugoje

Šie principai yra pamatinės taisyklės visoms teisės šakoms, pagrindai, kurių pažeisti negalima ir kurių ribose reiktų aiškinti tokius susidariusius teisinius iššūkius, kurių nereguliuoja imperatyvios teisės normos. Teisėtumo, sąžiningumo ir skaidrumo principus viena vertus galima būtų laikyti vienas kito sinonimais, nes visi užtikrina teisingą, sąžiningą, teisės aktus atitinkančią asmens duomenų apsaugą, tačiau kita vertus taip teigti nėra teisiškai tikslu bei teisinga, todėl toliau bus analizuojamas kiekvienas iš jų išskiriant esminius ypatumus taikant socialiniuose tinkluose.

Teisėtumo principas lingvistiniu metodu analizuojant reiškia – teisės aktus atitinkantis. Pabrėžtina, kad teisėtumo imperatyvus pobūdis numatytas tiek tarptautiniuose, tiek europiniuose, tiek nacionaliniuose teisės norminiuose šaltiniuose. Pagal BDAR visi trys principai įtvirtinti 5 str. 1 d. a p. Taip pat šis principas neišvengiamai susijęs su asmens duomenų tvarkymu, kur jo svarba laikoma prioritetu užtikrinant asmens duomenų apsaugą subjekto atžvilgiu. EBPO privatumo gairėse⁵⁰ įtvirtindamos duomenų rinkimo apribojimo principą, nustato reikalavimą, kad duomenys turi būti renkami teisėtomis ir sąžiningomis priemonėmis bei su duomenų subjekto žinia arba sutikimu tam tikrais atvejais (7str.). ES pagrindinių teisių chartija⁵¹ 8 str. teisėtumą forlumuoja būtinybės tikslo ir duomenų subjekto sutikimo gavimui aspektu: asmens duomenys turi būti tinkamai tvarkomi ir naudojami tik konkrečioms tikslams ir tik atitinkamam asmeniui sutikus ar kitais įstatymo nustatytais teisėtais pagrindais. Tą patį pasako ir BDAR 6 str. ir preambulės 40 p. pabrėždamas, kad nustatyti teisės pagrindą galima tik pagal ES teisę ar pagal ES valstybių narių teisę. Socialiniuose „Facebook“ ir „Instagram“ tinkluose duomenų privatumo politikoje⁵² nurodytos duomenų subjektų teisės: kiekvienas turi teisę susipažinti su surinktais jo asmens duomenimis bei teisę juos pataisyti; kiek tai būtina vykdyti „Facebook“ paslaugų sąlygas arba „Instagram“ paslaugų sąlygas; su vartotojo sutikimu, kurį bet kada galima atšaukti „Facebook“ ir „Instagram“ nustatymuose; kiek tai

⁵⁰1980 m. Ekonominio bendradarbiavimo ir plėtros organizacijos privatumo gairės [interaktyvus, žiūrėta 2019 m. rugsėjo 15 d.]. Prieiga per internetą: <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>>.

⁵¹ 2012 m. Europos Parlamento, Tarybos ir Komisijos paskelbta ES pagrindinių teisių chartija [interaktyvus, žiūrėta spalio 19 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12012P/TXT&from=LT>>.

⁵² Duomenų politika [interaktyvus, žiūrėta 2019 m. spalio 29 d.]. Prieiga per internetą: <<https://lt.facebook.com/help/instagram/155833707900388>>.

būtina laikytis „Facebook“ teisinių prievolių; apsaugoti gyvybinius vartotojų ir kitų interesus; kiek tai būtina užtikrinti viešuosius interesus; ir kiek tai būtina „Facebook“ ir vartotojų teisėtiems interesams, įskaitant socialinio tinklo interesą teikti naujoviškas, asmeniškai pritaikytas, saugias ir pelningas paslaugas savo naudotojams ir partneriams.

Sąžiningumo bendrasis teisės principas suvokiamas kaip žmogaus pamatinė vertybė, lemianti kiekvieno asmens moralumą ir elgesį. Asmens duomenų apsaugoje sąžiningumą principas apima duomenų valdytojų ir tvarkytojų pareigą tvarkyti duomenis sąžiningai. Šis principą sudaro objektyvusis ir subjektyvusis kriterijai. Pagal objektyvųjų kriterijų sąžiningumas suprantamas kaip elgesys, atitinkantis protingumo ir teisingumo principų reikalavimus – elgiamasi rūpestingai, apdairiai ir atidžiai. Subjektyvusis kriterijus nurodo asmens vidinę būklę konkrečioje situacijoje bei veikiamą subjektą apibūdinančias savybes kaip amžius, išsilavinimas (jei tai fizinis asmuo), veiklos pobūdį, verslo patirtį. Asmens sąžiningumui nustatyti šių kriterijų visumą privalu taikyti konkrečioje situacijoje.⁵³ Sąžiningumas yra bendrasis teisės principas. Sąžiningas subjektas yra toks, kuris veikia rūpestingai ir teisingai. Sąžiningumas reikalauja atidumo, rūpestingumo ir draudžia piktnaudžiauti teise. Sąžiningo asmens deklaruojami tikslai turi atitikti tuos tikslus, kurių jis iš tikrųjų siekia. Piktnaudžiavimu teise ir nesąžiningu elgesiu laikytinas ir naudojimasis teise ne pagal jos paskirtį ar tikslą.⁵⁴ Duomenų valdytojo elgesys laikomas neatitinkančiu sąžiningumo standarto, jeigu konstatuojamas duomenų valdytojo piktnaudžiavimo faktas. Piktnaudžiavimas – sąžiningumo priešingybė, o prielaidų piktnaudžiauti asmens duomenų teisinės apsaugos srityje itin gausu, nes duomenų valdytojas – tai subjektas, kurio žinioje yra asmens duomenys ir kuris vienintelis turi išsamią informaciją apie duomenų subjekto asmens duomenų tvarkymą.⁵⁵ Sąžiningumo principas pasireiškia per tikslo apribojimą principą: pagal BDAR 5 str. 1 d. b p. asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu. Asmens duomenys negali būti toliau tvarkomi ne pagal anksčiau apibrėžtą tikslą. Pažymėtina, kad sąžiningumo principas dažnai taikomas kartu su skaidrumo principu. Visuotinai pripažįstama, kad skaidrumas, kaip viešosios valdžios institucijų ir pareigūnų veiklos principas, suponuoja informacijos sklaidą ir komunikavimą, atvirumą ir viešumą (tiek, kiek tai nekenkia kitoms teisės saugomoms vertybėms), atskaitingumą atitinkamai bendruomenei ir sprendimus priimančių pareigūnų atsakomybę už tuos sprendimus, taip

⁵³ Lietuvos Aukščiausiojo teismo Civilinių bylų skyriaus kolegija. 2013 m. birželio 19 d. D.J v. V.J ir J.B, Nr. 3K-3-336/2013.

⁵⁴ Lietuvos vyriausiojo administracinio teismo teisėjų kolegija. 2017 m. lapkričio 21 d. S.F v. Vilniaus miesto savivaldybės administracija, Nr. AS-1003-756/2017.

⁵⁵ PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai*: daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013, p.111.

pat tai, kad priimami sprendimai turi būti pagrįsti, aiškūs, kad juos, iškilus reikalui, būtų galima racionaliai motyvuoti; kiti asmenys turi turėti galimybę tuos sprendimus nustatytą tvarka ginčyti. Skaidrumas sietinas su dalyvaujama demokratija, informacijos laisve, galimybe piliečiams ir kitiems asmenims kritikuoti valdžios įstaigų veiklą.⁵⁶ Asmens duomenų apsaugoje šios pareigos taikomos duomenų valdytojui užtikrinti duomenų subjekto teises pagal BDAR 12 str. 1 d. Duomenų valdytojas imasi tinkamų priemonių, kad visą BDAR 13 ir 14 straipsniuose nurodytą informaciją ir visus pranešimus pagal 15–22 ir 34 straipsnius, susijusius su duomenų tvarkymu, duomenų subjektui pateiktą glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba, ypač jei informacija yra konkrečiai skirta vaikui. Informacija pateikiama raštu arba kitomis priemonėmis ir prireikus elektronine forma. Duomenų subjekto prašymu informacija gali būti suteikta žodžiu, jeigu duomenų subjekto tapatybė įrodoma kitomis priemonėmis. „Glausta, skaidri, suprantama ir lengvai prieinama forma“ reiškia, kad duomenų valdytojai turėtų pateikti informaciją greitai ir glaustai. Ši informacija turėtų būti aiškiai atskirta nuo kitos su privatumu nesusijusios informacijos. Reikalavimas, kad informacija būtų suprantama, reiškia, kad ją turėtų suprasti vidutinis numatytos auditorijos narys. Valdytojas pirmiausia turi nustatyti numatytą auditoriją ir išsiaiškinti vidutinio asmens supratimo lygį. Kadangi numatoma auditorija vis dėlto gali skirtis nuo tikrosios auditorijos, duomenų valdytojas taip pat turėtų reguliariai tikrinti, ar informacija vis dar pritaikyta tikrajai auditorijai (ypač ten, kur ją sudaro vaikai), jei reikia - pakeisti. Šiose nuostatose apibrėžto skaidrumo principo esmė yra ta, kad duomenų subjektas turėtų sugebėti iš anksto nuspręsti, kokia duomenų tvarkymo apimtis ir kokios galimos pasekmės. Pabrėžtina, kad duomenų valdytojai turėtų ne tik pateikti nurodytą informaciją pagal BDAR 13 ir 14 straipsnius, bet ir atskirai aiškiai išdėstyti, kokios galimos ir labiausiai tikėtinos duomenų tvarkymo pasekmės - kokį poveikį duomenų subjektui iš tikrųjų turės konkretus duomenų tvarkymas, aprašytas privatumo patvirtinime / pranešime. Toks duomenų tvarkymo pasekmių

⁵⁶ Lietuvos Respublikos Konstitucinis teismas. 2008 m. sausio 22 d. nutarimas dėl Lietuvos Respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl priėmimo į valstybės tarnautojo pareigas tvarkos patvirtinimo“ (2002 m. Birželio 24 d., 2002 m. Rugsjūčio 29 d., 2003 m. Birželio 3 d., 2003 m. Lapkričio 25 d., 2005 m. Spalio 28 d. Redakcijos) patvirtintos priėmimo į valstybės tarnautojo pareigas tvarkos atitikties lietuvių respublikos konstitucijai, lietuvių respublikos valstybės tarnybos įstatymo 3 straipsnio (2002 m. Balandžio 23 d. Redakcija) 1 daliai, dėl lietuvių respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2006 m. Birželio 28 d. Redakcija) patvirtinto konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties lietuvių respublikos konstitucijai, lietuvių respublikos valstybės tarnybos įstatymo 3 straipsnio (2002 m. Balandžio 23 d., 2007 m. Birželio 7 d. Redakcijos) 1 daliai, taip pat dėl lietuvių respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2007 m. Rugsėjo 26 d., 2007 m. Gruodžio 12 d. Redakcijos) patvirtinto konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo atitikties lietuvių respublikos konstitucijai, lietuvių respublikos valstybės tarnybos įstatymo 3 straipsnio (2007 m. Birželio 7 d. Redakcija) 1 daliai.

aprašymas neturėtų būti grindžiamas tik minimaliausių pasekmių rizika, duomenų valdytojas privalo nurodyti, kokį didžiausias neigiamas poveikis gali kilti pagrindinėms duomenų subjektų teisėms. „Lengvai prieinama“ - duomenų subjektas neturėtų ieškoti informacijos, turi būti iš karto aišku, kur galima rasti šią informaciją, pavyzdžiui, tiesiogiai ją pateikiant, susiejant su ja, aiškiai nurodant ją (pvz., naudojant internetinį slapta privatumą). ES 29 str. darbo grupė rekomenduoja asmens duomenų rinkimo metu internetiniame puslapyje sukurti aiškia nuorodą dėl privačių duomenų panaudojimo, arba šią informaciją pateikti tame pačiame puslapyje.⁵⁷ Socialiniuose tinkluose dažniausiai informacija apie duomenų rinkimą patalpinama nustatymuose, prie privatumo nustatymų arba duomenų politikos. „Aiškia ir suprantama kalba“ - informacija turėtų būti teikiama kuo paprasčiau, vengiant sudėtingų sakinių ir kalbos struktūrų. Informacija turėtų būti konkreti ir tiksli, ji neturėtų būti formuluojama abstrakčiai ar dviprasmiškai, be jokių interpretacijų galimumo. Visų pirma, duomenų panaudojimo tikslai ir teisinis pagrindas bei asmens duomenų tvarkymas turėtų būti aiškūs. Pvz.: Šios frazės nėra pakankamai aiškios tvarkymo tikslams: „Mes galime naudoti jūsų asmens duomenis kurdami naujas paslaugas“ (nes neaišku, ką paslaugos yra ar kaip duomenys padės jas plėtoti); „Mes galime naudoti jūsų asmeninius duomenis tyrimų tikslais (nes neaišku kokie tyrimų tai reiškia); ir „Mes galime naudoti jūsų asmens duomenis siūlydami individualizuotas paslaugas“ (nes neaišku ką reiškia personalizavimas).⁵⁸ Tokie galimi nustatyti tikslai gali būti pagrindu asmens tapatybės vagystei, finansiniai nuostoliams, verslo ar įsidarbinimo galimybių praradimas ir fizinė žala⁵⁹.

Socialiniuose tinkluose teisėtumo, sąžiningumo bei skaidrumo principai pasireiškia per duomenų tvarkymo nustatytus tikslus, per patį duomenų tvarkymą, duomenų saugumo ir duomenų subjektų užtikrinimo teises. Duomenų tikslai, kuriais planuojama tvarkyti asmens duomenis, turi būti aiškiai, suprantai ir prieinama forma pateikti socialinių tinklų vartotojams, kurie galėtų greitai ir be kitų pagalbos susirasti, kam ir kokiems tikslams duomenys yra tvarkomi (plačiau apie duomenų tvarkymo tikslus bus analizuojama kitame skyriuje). Duomenys turi būti tvarkomi sąžiningai, skaidriai ir teisėtai, pvz.: socialinių tinklų valdytojas nusprendė surinktus duomenis ir panaudoti kitu tikslu nei buvo iki tol naudojami – tiesioginės rinkodaros, tokiu atveju socialinių tinklų valdytojas privalo

⁵⁷ 2017 m. ES 29 str. darbo grupės gairės dėl skaidrumo [interaktyvus, žiūrėta 2019 m. spalio 18 d.]. Prieiga per internetą: <https://iapp.org/media/pdf/resource_center/wp29-transparency-12-12-17.pdf>.

⁵⁸ *Ibid.*, p. 9.

⁵⁹ 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

pranešti ir paprašyti sutikimo socialinio tinklo vartotojo, priešingu atveju, tai jau būtų asmens duomenų apsaugos pažeidimas. Taip pat socialinio tinklo duomenų valdytojas privalo duomenis saugoti, tai, reiškia, kad jokie kiti asmenys neturi teisės prie asmens duomenų prieigos, duomenų valdytojas privalo imtis visų techninių ir organizacinių priemonių tam užtikrinti. Taip pat duomenų subjektas – socialinių tinklų vartotojas turi teisę žinoti viską apie savo duomenų tvarkymą, o duomenų valdytojas turi pareigą informuoti. Sužinojus, kad duomenys pasikeitę, juos patikslinti ir taip pat informuoti vartotoją. Teisėtumo, sąžiningumo ir skaidrumo principai yra pamatinės vertybės ir ribos, kuriomis privalu užtikrinti duomenų apsaugą pagal BDAR. Plačiau apie kiekvieną iš išvardintų BDAR reikalavimų bus aptarta kituose skyriuose.

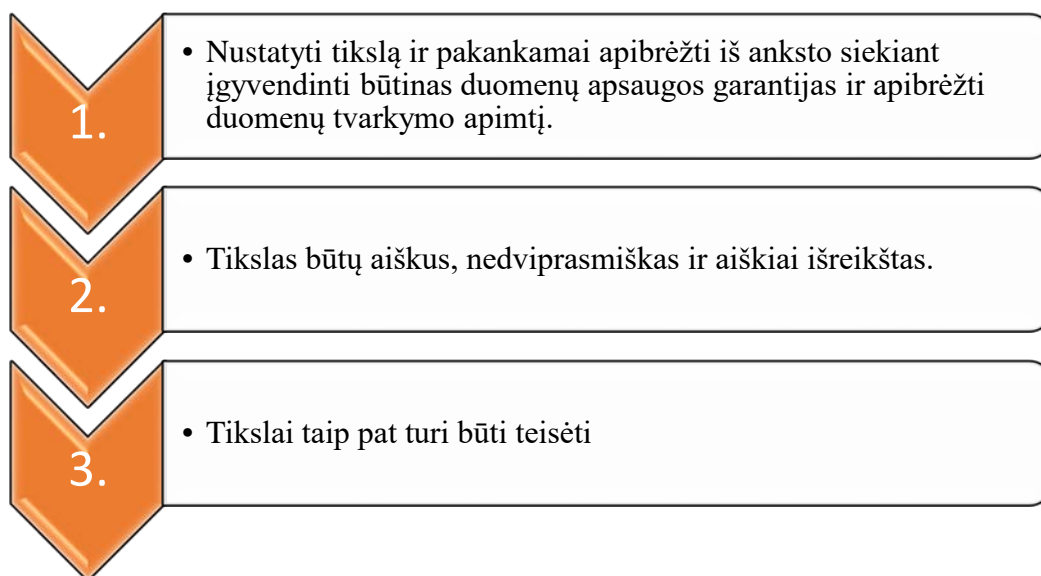
3.2 Duomenų tvarkymo tikslo apribojimo principo įgyvendinimas socialiniuose tinkluose

Šis principas, kuris reglamentuotas BDAR 5 str. 1 d. b p. asmens duomenys renkami nustatytais, aiškiai apibrėžtais bei teisėtais tikslais ir toliau netvarkomi su tais tikslais nesuderinamu būdu; tolesnis duomenų tvarkymas archyvavimo tikslais viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais pagal 89 straipsnio 1 dalį nėra laikomas nesuderinamu su pirminiais tikslais, gali atrodyti, jog yra visiškai naujas principas teisėje, tačiau taip nėra, nes jis glaudžiai susijęs su teise į privatumą (šiame skyriuje nebus analizuojamas santykis su privatumu, nes plačiau aptarta ankstesniame 2.3 skyriuje). Toliau bus detalizuojamas duomenų tvarkymo tikslo apribojimo principas.

Asmens duomenys turi būti renkami aiškiais ir apibrėžtais tikslais. Rinkimo tikslai turi būti aiškiai apibrėžti ne tik asmenų, atsakingų už duomenų rinkimą, mintyse. Kitaip tariant, jie turi būti aiškiai atskleisti, paaiškinti ar išreikšti tam tikra suprantama forma. Taikant duomenų apsaugos įstatymus pirmiausia reikia įsitikinti, kad tikslas yra konkretus, aiškus ir teisėtas. Tai yra būtina sąlyga siekiant įvykdyti kitus duomenų kokybės reikalavimus, įskaitant tinkamumą, aktualumą ir proporcingumą (Direktyvos 95/46/EB 6 straipsnio 1 dalies c punktas), tikslumą ir išsamumą (10 straipsnis). 6 straipsnio 1 dalies d punktas) ir reikalavimai dėl išlaikymo trukmės (6 straipsnio 1 dalies e punktas). Tais atvejais, kai nuo pat pradžių egzistuoja skirtingi tikslai ir tuo pačiu tikslu renkami ir apdorojami skirtingų rūšių duomenys, duomenų kokybės reikalavimų kiekvienam tikslui privalu laikytis atskirai. Jei asmens duomenys toliau tvarkomi kitu tikslu: turi būti nurodytas naujas tikslas (-ai) (6 straipsnio 1 dalies b punktas), ir turi būti užtikrinta, kad būtų laikomasi ir visų duomenų kokybės reikalavimų (6 straipsnio 1 dalies

a – e punktai) patenkintas naujais tikslais.⁶⁰ Duomenų tvarkymo principas susijęs su duomenų tvarkymo skaidrumu, teisiniu apibrėžtumu ir nuspėjamumu. Tarp skaidrumo ir tikslo apibrėžimo yra glaudus ryšys. Skaidrumas užtikrina nuspėjamumą ir leidžia vartotojui valdyti. Nuspėjamumas pasižymi per tikslą, jei yra pakankamai konkretus ir aiškus, asmenys žinos, ko tikėtis: duomenų tvarkymo būdas bus nuspėjamas. Tai suteikia teisinį tikrumą duomenų subjektams, taip pat tiems, kurie tvarko asmens duomenis duomenų valdytojo vardu. Nuspėjamumas taip pat yra svarbus vertinant tolesnio duomenų tvarkymo veiklos suderinamumą. Apskritai tolesnis tvarkymas negali būti laikomas nuspėjamu, jei jis nėra pakankamai susijęs su pirminiu tikslu ir neatitinka pagrindų duomenų subjektų lūkesčių.⁶¹ Taigi, vertinant duomenų tvarkymo tikslo apribojimo principą išskirti trys esminiai imperatyvūs reikalavimai (žr. į 2 lentelę) – iš anksto nustatyti tikslą, kuris būtų aiškiai apibrėžtas ir teisėtas.

3 lentelė. Duomenų tvarkymo tikslo apibrėžtis



Šaltinis: Sudaryta remiantis: autorės pagal ES 29 str. ES darbo grupės tikslo apribojimo gaires.

Prieiga per internetą:

<https://ec.europa.eu/justice/article29/documentation/opinionrecommendation/files/2013/wp203_en.pdf>.

Reikalavimas dėl tikslo nustatymo iš anksto numato, kad asmens duomenys turi būti renkami nurodytais tikslais. Duomenų valdytojas turi atidžiai įvertinti, koku tikslu ar kokiais tikslais bus naudojami asmens duomenys, draudžiama rinkti asmens duomenis, kurie nėra būtini, pakankami ar svarbūs tam tikslui pasiekti. Tikslo apibrėžimas yra teisinė

⁶⁰ 2013 m. balandžio 2 d. ES 29 str. darbo grupės nuomonė Nr. 03/2013 dėl tikslo apribojimo Nr. WP203 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

⁶¹ *Ibid.*

prievolė, sukurta siekiant apsaugoti asmeninius duomenis nustatant ne vėliau kaip iki asmens duomenų rinkimo laiko. Duomenų valdytojo atskaitomybės pareiga numato pagal BDAR 5 str. 2. , kad duomenų valdytojas turi sugebėti bei prirėikus įrodyti, kad tikslas yra aiškiai, tiksliai iš anksto teisėtai apibrėžtas bei asmens duomenys nebus panaudojami su tikslu nesuderinamu būdu.

Reikalavimas dėl tikslo suformulavimo aiškiai reiškia, kad tikslas turi būti atskleistas lengvai suprantama forma ir nekelti jokių abejonių dėl turinio. Tikslų apibrėžimas visų pirma turi būti išreikštas taip, kad jį vienodai suprastų ne tik duomenų valdytojas (įskaitant visus susijusius darbuotojus) bet ir suinteresuotieji asmenys: duomenų subjektai, duomenų apsaugos institucijos, duomenų tvarkytojai. Ypatingai reikėtų kiek tai įmanoma užtikrinti, kad bet koks tikslo apibūdinimas būtų pakankamai aiškus visiems dalyviams, neatsižvelgiant į skirtingą jų kultūrinę / kalbinę pagrindą, supratimo lygį ar specialiuosius poreikius.

Tikslai turi būti teisėti – šis reikalavimas susijęs su duomenų tvarkymo teisėtumo kriterijais BDAR 7 str. , tačiau neapsiriboja šia apimtimi. Tikslo teisėtumo kriterijus siejamas ne tik su asmens duomenų apsaugos teise, teisėtumas apima taikomus įstatymus, tokius kaip darbo teisė, sutarčių teisė, vartotojų apsaugos įstatymai ir pan. Teisėtumo reikalavimas reiškia, kad tikslai turi būti "laikantis įstatymų", esančių plačiausia prasme. Tai apima visus bendrosios teisės norminius aktus, pirminius ir antrinius įstatymus, savivaldybių dekretus, teisinius precedentus, konstitucinius principus, pagrindines teises, kitus teisės principus, taip pat teismų praktiką. Gali būti atsižvelgiama į kitus elementus, tokius kaip papročiai, elgesio kodeksai, etikos kodeksai, sutartiniai susitarimai ir bendras bylos kontekstas bei faktai, ar konkretus tikslas yra teisėtas. Tai apims pagrindinių duomenų valdytojo ir duomenų subjektų santykių pobūdį, neatsižvelgiant komerciniais ar kitokiais.

Socialinių tinklų valdytojai turi pareigą informuoti vartotojus apie jų tapatybę ir pateikti išsamią ir aiškią informaciją apie tikslus ir visus būdus, kuriais jie ketina tvarkyti asmens duomenis, taip pat socialinių tinklų valdytojai turėtų teikti informaciją ir tinkamai įspėti vartotojus apie privatumo riziką, kai jie įkelia duomenis į socialinius tinklus. Vartotojams turėtų pranešti, kad nuotraukos ar informacija apie kitus asmenis turėtų būti įkeliami tik gavus asmens sutikimą kitaip tariant socialinių tinklų vartotojas norėdamas naudoti informaciją apie kitus asmenis, privalo gauti jų sutikimą. Savališkai dalinantis ir platinantis socialinėje erdvėje informaciją apie tokį asmenį, galima pažeisti BDAR duomenų subjekto

teisę dėl sutikimo nedavimo asmens duomenų tvarkymui.⁶² Taip pat pabrėžtina, kad socialinių tinklų vartotojai turi būti informuoti, kai jų duomenys renkami tiesioginės rinkodaros tikslais bei nurodyti, kokie konkrečiai duomenys renkami, nes šiandieninime technologijų ir globalizacijos pasaulyje socialiniai tinklai grindžiami ne bendravimu, o verslo modeliu, kuris remiasi tiesiogine rinkodara.⁶³ Apsilankymas interneto svetainėje kompiuterio naudotojo duomenis (pvz., IP adresas, nustatyta kalba, laiko zona, programinė įranga, slapukai ir kt.) siunčia kelioms skirtingose valstybėse veikiančioms rinkodaros, reklamos ir kita veikla besiverčioms bendrovėms⁶⁴, todėl duomenų tvarkymo tikslas yra vienas iš būdų apsaugoti asmens duomenis nuo neteisėto jų tvarkymo.

Taigi, duomenų tvarkymo tikslo apribojimo principas yra vienas iš svarbiausių asmens duomenų apsaugos principų įgyvendinant teisėtą duomenų tvarkymą socialiniuose tinkluose. Jei prieš pradėdant tvarkyti asmens duomenis, šis principas bus įgyvendintas netinkamai t.y., tikslas nebus aiškus, suformuluotas abstrakčiai ar neteisėtas, tai didelė rizika susidurti su neteisėtu duomenų tvarkymu tiesioginės rinkodaros tikslais arba perteklinių duomenų panaudojimu socialiniuose tinkluose, apie kuriuos bus kalbama kitame skyriuje.

3.3 Duomenų kiekio mažinimo pareiga

Šis principas susijęs su duomenų tvarkymo tikslo apribojimo principu tuo, kad tikslui pasiekti reikia rinkti tik tam įgyvendinti susijusius asmens duomenis, o ne visus, kokius tik įmanoma. Kitaip tariant asmens duomenys turėtų būti tvarkomi tik tuomet, kai asmens duomenų tvarkymo tikslo pagrindai negalima pasiekti kitomis priemonėmis. Jeigu įmanoma, geriau naudoti anoniminius duomenis⁶⁵. Pagal BDAR 5 str. c) asmens duomenys turi būti: adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi. ET duomenų apsaugos konvencija reikalauja, kad duomenys būtų proporcingi (5str.1d.). EBPO privatumo gairės reikalauja, kad duomenys būtų būtini, atsižvelgiant į duomenų tvarkymo tikslus (8str.).

Svarbu pabrėžti, kad duomenų kiekio mažinimo pareiga kyla iš proporcingumo principo. Konstitucinis Teismas yra pažymėjęs, kad proporcingumo principas – tai konstitucinis principas, konstitucinio teisinės valstybės principo dalis, reiškiantis tai, kad įstatyme

⁶² 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

⁶³ CIVILKA M.; ŠLAPIMAITĖ L. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, p.

⁶⁴ *Ibid.*, p. 128.

⁶⁵ Oficiali Europos Sąjungos svetainė [interaktyvus, žiūrėta 2019 m. spalio 26 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-much-data-can-be-collected_lt>.

numatytos priemonės turi atitikti teisėtus ir visuomenei svarbius tikslus, kad šios priemonės turi būti būtinos minėtiems tikslams pasiekti ir jos neturi varžyti asmens teisių ir laisvių akivaizdžiai labiau negu reikia šiems tikslams pasiekti.⁶⁶ Konstitucinio Teismo nuomone, proporcingumo principas, be kita ko, turi būti taikomas, reglamentuojant su teisine atsakomybe susijusius klausimus. Pasak Teismo, konstituciniai teisingumo, teisinės valstybės principai suponuoja tai, kad už teisės pažeidimus valstybės nustatomos poveikio priemonės turi būti proporcingos (adekvačios) teisės pažeidimui, jos turi atitikti siekiamus teisėtus ir visuotinai svarbius tikslus; asmens teisės gali būti apribotos tik tiek, kiek yra būtina viešiesiems interesams ginti, ir asmuo neturi būti varžomas akivaizdžiai labiau negu reikia šiems tikslams pasiekti; tarp siekiamo tikslo nubausti teisės pažeidėjus, užtikrinti teisės pažeidimų prevenciją ir pasirinktų priemonių šiam tikslui pasiekti turi būti teisinga pusiausvyra (proporcingumas); taip pat turi būti išlaikoma teisinga pusiausvyra tarp visuomenės ir asmens interesų, kad būtų išvengta nepagrįsto asmens teisių ribojimo.⁶⁷ Asmens duomenų teisėje proporcingumo santykis su duomenų kiekio mažinimo principu pasižymi per duomenų tvarkymo tikslą ir duomenų apimties santykį.⁶⁸ Kitaip tariant, nebus galima taikyti duomenų kiekio mažinimo principo, jei nebus iš anksto teisėtais pagrindais, aiškiai, tiksliai, nedviprasmiškai suformuluotas tikslas. Pavyzdžiui, jei nusistatomas tikslas rinkti asmens duomenis reklaminių el. pašto laiškų siuntimui, tam nėra reikalingi asmenų telefono numeriai, todėl telefono numerių rinkti nereiktų, kadangi jie nėra reikalingi nustatytam tikslui pasiekti.

Įvertinus duomenų kiekio mažinimo principo sąsają su duomenų tvarkymo tikslo apribojimo bei proporcingumo principais santykį, išskirtini 3 elementai: būtinumo, adekvatumo, tinkamumo.⁶⁹ Būtinumo kriterijus įtvirtintas BDAR preambulės 39 p. „Asmens duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrindai negalima pasiekti kitomis priemonėmis.“ Duomenys turėtų būti naudojami tik tada, kai to tikslo nėra galimybės pasiekti kitomis priemonėmis nepanaudojant tų asmens duomenų, asmens duomenų panaudojimas turėtų būti kaip paskutinė galimybė pasiekti

⁶⁶ Lietuvos Respublikos Konstitucinio Teismo. 2010 m. birželio 29 d. nutarimas dėl Lietuvos Respublikos teisėjų valstybinių pensijų įstatymo 5, 6 straipsnių, Lietuvos Respublikos valstybinių pensijų įstatymo 3 straipsnio 3 dalies (2009 m. gruodžio 8 d. redakcija), Lietuvos Respublikos socialinių išmokų perskaičiavimo ir mokėjimo laikinojo įstatymo 1 straipsnio 2 dalies 1 punkto, 16 straipsnio 4 dalies atitikties Lietuvos Respublikos Konstitucijai, Nr. 134-6860.

⁶⁷ Lietuvos Respublikos Konstitucinis teismas. 2011 m. sausio 31 d. nutarimas dėl Lietuvos Respublikos civilinio kodekso 4.103 straipsnio (2006 m. spalio 17 d. redakcija) 3 dalies ir Lietuvos Respublikos statybos įstatymo 28 straipsnio (2006 m. spalio 17 d., 2009 m. lapkričio 19 d. redakcijos) 3 dalies atitikties Lietuvos Respublikos Konstitucijai, Nr. 14-602.

⁶⁸ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registru centras, 2019.

⁶⁹ *Ibid.*, p. 122.

tiksliui, o ne teikiant prioritetą neapmaščius duomenų valdytojui kitokio būdo. Kitas labai svarbus ir reikšmingas elementas tinkamumo – tiksliui pasiekti, duomenys turi būti renkami tik tokie, kurie susiję su duomenų valdytojų tikslu, priešingu atveju, tai jau būtų pažeidimas. Adekvatumo kriterijus numato jau anksčiau aptartą šiame skyriuje proporcingumo principo taikymą, tai reiškia, kad asmens duomenys turi būti renkami konkrečiam tikslui pasiekti, priemonės turi būti atitinkančios tikslą, taip pat duomenų saugojimo trukmė neturi būti ilgesnė nei duomenų panaudojimo tam tikslui trukmė bei kokiais būdais tvarkomi duomenys, kokiais asmens duomenų tvarkymo veiksmais ir t.t.

Įvertinus duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo, teisėtumo, sąžiningumo, teisingumo principus ir BDAR reguliavimą dėl asmens duomenų tvarkymo galima teigti, kad prieš pradėdant teisėtai pradėti tvarkyti asmens duomenis privaloma atlikti duomenų valdytojui šiuo 4 žingsnius (žr į lentelę nr. 2).

4 lentelė. **Pasiruošimas asmens duomenų tvarkymui**



Šaltinis: Sudaryta remiantis: autorės pagal Karolį Sadauską. Prieiga per internetą: <www.linden.lt>.

Pirmas žingsnis – nustatyti tikslą, kuriam renkate asmens duomenis. BDAR reikalauja, kad visi duomenys būtų kaupiami konkrečiam tikslui, kurį teks atskleisti fiziniam asmeniui, kurio duomenis renkate. Papildomai pažymėtina, kad nusistačius tikslą, jo nebus galima pakeisti. Taip pat, sukauptų duomenų, su retomis išimtimis, nebus galima pradėti naudoti kitiems tikslams. Tokie veiksmai dažniausiai reikš BDAR reikalavimų pažeidimą. Nustatant tikslą, kuriam bus renkami asmens duomenis, svarbiausia jį aiškiai apibrėžti bei įsitikinti, kad jis neprieštaruja įstatymams. Antras žingsnis – nusistatyti kokių duomenų reikia išsikeltam tikslui įgyvendinti. Duomenų apsaugos reguliavime labai svarbią vietą

užima duomenų kiekio mažinimo principas. Šis principas reiškia, kad reikėtų rinkti tik tokius asmens duomenis, kurių reikia nusistatytam tikslui pasiekti. Trečias žingsnis – nusistatyti duomenų saugojimo terminus. Duomenų negalima saugoti visiškai neribotą laikotarpį. Vadovaujantis saugojimo trukmės apribojimo principu, duomenis galima saugoti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi. Atsižvelgiant į tai, reikėtų pasirinkti tokius duomenų saugojimo terminus, kurie nepažeistų fizinių asmenų teisių. Papildomai pažymėtina, kad apie surinktų duomenų saugojimo terminą bus privaloma pranešti fiziniams asmenims. Ketvirtas žingsnis – duomenų tvarkymo teisėto pagrindo pasirinkimas pagal BDAR 6 str. nustato šešias teisėtumo sąlygas asmens duomenų tvarkymui: a) duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais; b) tvarkyti duomenis būtina siekiant įvykdyti sutartį, kurios šalis yra duomenų subjektas, arba siekiant imtis veiksmų duomenų subjekto prašymu prieš sudarant sutartį; c) tvarkyti duomenis būtina, kad būtų įvykdyta duomenų valdytojui taikoma teisinė prievolė; d) tvarkyti duomenis būtina siekiant apsaugoti gyvybinius duomenų subjekto ar kito fizinio asmens interesus; e) tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas; f) 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.⁷⁰ Svarbu pabrėžti, kad šie žingsniai yra imperatyviai privalomi norint išvengti asmens duomenų teisės pažeidimų, tačiau svarbu žinoti, kad duomenis prieš pradėdant teisėtai tvarkyti, reiktų informuoti duomenų subjektą dėl asmens duomenų panaudojimo, gauti jo sutikimą. Jei šie žingsniai bus įvykdyti teisėtai, teisingai ir sąžiningai duomenų valdytojo, tuomet maža tikimybė susidurti su perteklinių duomenų rizika.

Norint užtikrinti duomenų kiekio mažinimo principo efektyvumą, tiksliau tariant – būtinumo kriterijų, skatinama duomenis nuasmeninti. Duomenų nuasmeninimas ir anoniminiai duomenys nėra tapačios sąvokos. BDAR preambulės 26 p. „, 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 šis reglamentas netaikomas tokios anonimiškos

⁷⁰ 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) [interaktyvus, žiūrėta 2019 m. rugsėjo 22 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:32016R0679&from=LT>>.

informacijos tvarkymui, įskaitant statistiniais ar tyrimų tikslais“. Nuasmeninta informacija priešingai nei anoniminė yra susijusi su asmeniu, tačiau norint, kad asmens duomenys taptų nuasmenintais reikia pašalinti tiek duomenų elementų, kad nebūtų galima nustatyti duomenų subjekto.⁷¹ Sprendžiant, ar galima nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visas priemones, pavyzdžiui, išskyrimą, kurias asmens tapatybei tiesiogiai ar netiesiogiai nustatyti, pagrįstai tikėtina, galėtų naudoti duomenų valdytojas ar kitas asmuo. Įsitikinant, ar tam tikros priemonės, pagrįstai tikėtina, galėtų būti naudojamos siekiant nustatyti fizinio asmens tapatybę, reikėtų atsižvelgti į visus objektyvius veiksnius, pavyzdžiui, sąnaudas ir laiko trukmę, kurių prireiktų tapatybei nustatyti, turint omenyje duomenų tvarkymo metu turimas technologijas bei technologinę plėtrą.

Socialiniuose tinkluose siekiant išvengti perteklinių duomenų panaudojimo būtina tinkamai įvertinti pažeidžiamą vartotojų grupę – vaikus. Užsiregistruoti pvz.: „Facebook“ socialiniame tinkle galima nuo 13 metų. Vaiko asmens duomenų tvarkymas yra teisėtas tik tuo atveju, jei vaikas yra bent 16 metų amžiaus. Kai vaikas yra jaunesnis nei 16 metų, toks tvarkymas yra teisėtas tik tuo atveju, jeigu tą sutikimą davė arba tvarkyti duomenis leido vaiko tėvų pareigų turėtojas, ir tokiu mastu, koku duotas toks sutikimas ar leidimas (BDAR 8 str. 1 d.). Tai reiškia, kad tokie socialinių tinklų vartotojai yra nepilnamečiai už kuriuos atsakingi tėvai. Vaikams reikia ypatingos jų asmens duomenų apsaugos, nes jie gali nepakankamai suvokti su asmens duomenų tvarkymu susijusius pavojus, pasekmes ar apsaugos priemones ir savo teises. Tokia ypatinga apsauga visų pirma turėtų būti vaikų asmens duomenų naudojimui rinkodaros, virtualios asmenybės ar vartotojo profilio sukūrimo tikslais ir su vaikais susijusių asmens duomenų rinkimui naudojantis vaikui tiesiogiai pasiūlytomis paslaugomis. Tėvų pareigų turėtojo sutikimo neturėtų būti reikalaujama tiesiogiai vaikui teikiant prevencijos ar konsultavimo paslaugas (BDAR preambulės 38 p.). Informacija ir pranešimai, kai duomenų tvarkymas orientuotas į vaiką, turėtų būti suformuluoti vaikui lengvai suprantama aiškia ir paprasta kalba (BDAR preambulės 58 p.). Taigi, žinant tokią vaiko padėtį ir faktą, kad socialiniais tinklais naudojasi didelė dalis vartotojų jaunesnių nei 13 m.⁷², būtina socialinių tinklų valdytojams visomis priemonėmis ne tik įvertinti būtinumą, adekvatumą ir tinkamumą naudotis duomenimis apie vaiką, bet ir papildomas priemones siekiant tinkamai apsaugoti duomenis

⁷¹ 2014 m. birželio 14 d. ES 29 str. darbo grupės nuomonė Nr. 0829/14 dėl nuasmeninimo metodų [interaktyvus, žiūrėta 2019 m. spalio 30 d.]. Prieiga per internetą: <<https://www.pdpjournals.com/docs/88197.pdf>>.

toliau nebus nagrinėjami išsamiau nuasmeninimo metodai, nes nepatenka į magistro darbo rašymo apimtį.

⁷² 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

žinant riziką dėl realaus amžiaus neatitikimo bei būtinybę informuoti tėvus apie vaiką iki 16 m. naudojamus duomenis socialiniuose tinkluose.

Taigi, duomenų kiekio mažinimo pareiga užtikrina, kad duomenų valdytojai prieš pradėdami tvarkyti asmens duomenis nusistatytų ir apibrėžtų būtinumo, adekvatumo, tinkamumo kriterijus ir tik juos tinkamai įvykdę išvengs perteklinių duomenų panaudojimo rizikos ir taip tinkamai užtikrins pagal BDAR numatytą duomenų subjekto asmens duomenų apsaugos taikymą. Privalu skirti ypatingą dėmesį vaikams ir nepilnamečiams socialinių tinklų vartotojams, kuriems pateikti su duomenų tvarkymo tikslu susijusią informaciją būtina esant tėvų sutikimui iki 16 m. Tarkomi asmens duomenys turi būti tikslūs ir prireikus atnaujinami, todėl toliau bus aptariamas duomenų tikslumo principo privalomumas.

3.4 Duomenų tikslumo principo privalomumas

Duomenų tikslumo reikalavimas reiškia, kad asmens duomenys turi būti tikslūs ir prireikus atnaujinami. Svarbu pabrėžti, kad tikslumo principas ir jau išanalizuotas duomenų tvarkymo tikslo apribojimo principas (žr. į 3.2 poskyrį) nėra visiškai tapačios sąvokos, bet susijusios. Pagal BDAR 5 str. 1 d. d p. asmens duomenys tikslūs ir prireikus atnaujinami; turi būti imamasi visų pagrįstų priemonių užtikrinti, kad asmens duomenys, kurie nėra tikslūs, atsižvelgiant į jų tvarkymo tikslus, būtų nedelsiant ištrinami arba ištaisomi.

BDAR neapibrėžia duomenų tikslumo sąvokos, tačiau tai nesuteikia pareigos netaikyti šio principo, nes šio principo esminės nuostatos kaip teisė ištaisyti duomenis bei teisė į duomenų ištrynimą (teisė būti pamirštam)⁷³, reglamentuota per duomenų subjekto teises, kurios įtvirtintos BDAR 16 str. „Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištaisytų netikslus su juo susijusius asmens duomenis. Atsižvelgiant į tikslus, kuriais duomenys buvo tvarkomi, duomenų subjektas turi teisę reikalauti, kad būtų papildyti neišsamūs asmens duomenys, be kita ko, pateikdamas papildomą pareiškimą.“ Ir BDAR 17 str. „Duomenų subjektas turi teisę reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas ištrinti asmens duomenis, jei tai galima pagrįsti viena iš šių priežasčių:“. Priežastys gali būti tokios: asmens duomenys nėra reikalingi dėl numatyto tikslo, asmens duomenų subjektas atšaukia sutikimą, nes nebėra jokio teisinio pagrindo tolimesniam duomenų tvarkymui, asmens duomenų subjektas nesutinka su duomenų tvarkymu dėl su juo susijusių konkrečių priežasčių bei dėl tiesioginės rinkodaros, asmens duomenys buvo tvarkomi neteisėtai, asmens duomenys turi

⁷³ Guide to the general data protection [interaktyvus, žiūrėta 2019 m. spalio 30 d.]. Prieiga per internetą: <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>>.

būti ištrinti laikantis Sąjungos arba valstybės narės teisėje, kuri taikoma duomenų valdytojui, nustatytos teisinės prievolės, asmens domenys buvo surinkti informacinės visuomenės paslaugų siūlymo kontekste vaikui.

Duomenų tikslumą iš esmės reikėtų suprasti kaip duomenų ir faktinės, objektyvios tikrovės atitikties.⁷⁴ Asmens duomenų sąvoka išanalizuota 2.1 poskyryje, kuri reiškia, kad asmens duomenys tai informacija susijusi su fiziniu asmeniu, kurio tapatybė gali būti nustatyta. Pastebėtina, kad asmens duomenų samprata apima ir subjektyvaus pobūdžio nuomonę: nuomonė nebūtinai yra netikslūs asmens duomenys vien dėl to, kad asmuo su ja nesutinka, arba vėliau paaiškėja, kad ji neteisinga. Nuomonės pagal savo prigimtį yra subjektyvios ir neskirtos užrašyti faktinius dalykus. Tačiau tam, kad asmens duomenys būtų tikslūs, turi būti aišku, kad tai yra nuomonė ir, tam tikrais atvejais, kieno nuomonė ji yra. Jei paaiškėja, kad nuomonė buvo pagrįsta netiksliais duomenimis, taip pat turėtumėte užregistruoti šį faktą, kad įsitikintumėte, jog įrašai nėra klaidinantys.⁷⁵ Tačiau iš esmės nuomonės tikslumas negalėtų būti patikrintas. Kai kuriuose įrašuose, kurie gali atrodyti kaip nuomonės, nuomonėmis nelaikomi. Pavyzdžiui, daugelis finansų institucijų naudoja kredito reitingus, kad padėtų apsispręsti, ar suteikti kreditą. Kredito balas yra skaičius, apibendrinantis ankstesnę informaciją apie kreditą kredito ataskaitoje ir pateikiantis skaitinę prognozės riziką, susijusią su individualaus kredito suteikimu. Kredito balai yra paremti statistine asmenų asmeninių duomenų analize, o ne subjektyvia nuomone apie jų kreditingumą.⁷⁶ Duomenų tikslumas numato, kad naudojami duomenys turi būti aktualūs tikslui pasiekti, nes priešingu atveju duomenų valdytojas žinodamas, kad duomenys pasenę ir juos toliau naudotų, tai reikštų duomenų tikslumo principo pažeidimą išskyrus, jei duomenų subjektas su duomenų valdytoju būtų sutaręs dėl istorinio pobūdžio duomenų, tokiu atveju nereikalingas atnaujinimas.⁷⁷

Socialiniuose tinkluose vartotojai gali atnaujinti savo duomenis su kitomis programomis. Pavyzdžiui, vartotojai gali: skaityti ir siųsti žinutes į tinklą iš savo mobiliojo telefono; sinchronizuoti socialiniuose tinkluose savo draugų kontaktinius duomenis su jų adresų knyga, automatiškai atnaujinti jų būseną ar vietą socialiniame tinkle naudodamiesi kita svetaine. Asmens duomenys, kuriuos vartotojas perduoda registruodamiesi socialiniuose tinkluose, turėtų būti ištrinti, kai tik vartotojas arba socialinių tinklų duomenų

⁷⁴ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p. 124.

⁷⁵ Guide to the general data protection, p. 34. [interaktyvus, žiūrėta 2019 m. spalio 30 d.]. Prieiga per internetą: <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>>.

⁷⁶ *Ibid.*

⁷⁷ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019.

valdytojas nusprendžia tai padaryti. Tačiau, kai vartotojas atnaujina savo paskyrą socialiniame tinkle, informacija, kuri buvo ištrinta, neturi būti saugoma. Socialinių tinklų valdytojas turėtų pranešti vartotojams prieš imdamasis šių veiksmų bei privalo informuoti vartotojus apie saugojimo laikotarpius. Saugumo ir teisiniais sumetimais konkrečiais atvejais gali būti pagrįsta saugoti atnaujintus ar ištrintus duomenis bei socialinių tinklų paskyras nustatytą laikotarpį tam, kad būtų galima užkirsti kelią nusikalstamoms veikoms ir dėl viešojo intereso apsaugos.⁷⁸

Už duomenų tikslumo įgyvendinimą atsakomybė tenka duomenų valdytojui, kuris atsakingas už technines ir organizacines priemones duomenų tikslumui užtikrinti, o prireikus atnaujinti bei turi sugebėti įrodyti, kad tinkamai tai daro (atskaitomybės principas) BDAR 5 str. Taip pat duomenų valdytojas turi imtis visų būtinų organizacinių ir techninių priemonių įgyvendinant duomenų tikslumo principą vertindamas tokias aplinkybes kaip įgyvendinimo sąnaudos, duomenų tvarkymo pobūdis, tikslus ir pan. BDAR 25 str. 2 d. BDAR 15 str. 1 d. 1 p duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir toliau nurodyta informacija: a) duomenų tvarkymo tikslai; b) atitinkamų asmens duomenų kategorijos bei pagal 3 pastorėjo straipsnio d. duomenų valdytojas pateikia tvarkomų asmens duomenų kopiją. Duomenų tikslumo principas užtikrinamas ir per duomenų saugumo (vientisumo ir konfidencialumo) principą, kuris numato, kad asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo BDAR 5 str. 1 d. f p, 32 str. Pažymėtina, kad pareiga įgyvendinti tinkamas organizacines ir technines duomenų apsaugos priemones kyla tiek duomenų valdytojui, tiek duomenų tvarkytojui dėl tinkamo saugumo lygio nustatymo esant pavojui. BDAR 32 str. 2 d. preambulės 83 p. nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.

Taigi, įvertinus duomenų tikslumo principo privalomumą svarbu pabrėžti, kad duomenų tikslumo sąvoka nėra įvirtinta BDAR, tačiau įgyvendinama per duomenų subjekto teisių

⁷⁸ 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion_recommendation/files/2009/wp163_en.pdf>.

nuostatas dėl duomenų atnaujinimo ir dėl duomenų ištrynimo. Socialiniuose tinkluose vartotojų paskyrose ištrinta informacija neturi būti saugoma išskyrus dėl nusikalstamos veikos ar viešojo intereso apsaugos. Duomenų tikslumo principą padeda įgyvendinti duomenų saugumo ir atskaitomybės principai, kurie bus analizuojami sekančiame skyriuje.

3.5 Saugumo užtikrinimas ir atskaitomybės pareiga

Saugumo principas dar vadinamas duomenų konfidencialumo ir vientisumo principu. Pagal BDAR 5 str. 1 str. f p. asmens duomenys tvarkomi tokiu būdu, kad taikant atitinkamas technines ar organizacines priemones būtų užtikrintas tinkamas asmens duomenų saugumas, įskaitant apsaugą nuo duomenų tvarkymo be leidimo arba neteisėto duomenų tvarkymo ir nuo netyčinio praradimo, sunaikinimo ar sugadinimo. ET duomenų apsaugos konvencijos 7str.⁷⁹ „Automatizuotai kaupiamiems asmens duomenims apsaugoti turi būti imtasi tinkamų apsaugos priemonių, kurios neleisų jų netyčia ar neteisėtai sunaikinti, netyčia prarasti, neleistinai palikti juos prieinamus, keisti ar platinti“, EBPO privatumo gairių⁸⁰ 11str. numatyta analogiškai „Asmens duomenys turėtų būti apsaugoti pagrįstomis apsaugos priemonėmis nuo tokios rizikos kaip praradimas arba neteisėtos prieigos, duomenų sunaikinimo, naudojimo, modifikavimo ar atskleidimo“.

Kaip jau buvo minėta ankstesniame skyriuje pagal BDAR 32 str. pareiga dėl techninių ir organizacinių priemonių duomenų saugumui užtikrinta numatyta duomenų valdytojui bei duomenų tvarkytojui. Saugumo principas sudaro visumą šių principų: duomenų valdytojo ir tvarkytojo diskrecijos principas, pavojumi asmenims grįsto požiūrio (angl.*riskbasedapproach*) principas, duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo principas; duomenų saugumo priežiūros principas.⁸¹

Duomenų diskrecijos principas įtvirtintas BDAR preambulės 83 p. , kuris numato, kad tiek duomenų valdytojas, tiek duomenų tvarkytojas turi laisvę pasirinkti kokiomis priemonėmis užtikrinti duomenų saugumą neperžiangiant nustatytų ribų. Svarbu paminėti, kad BDAR nėra techninis informacinių technologijų reguliavimo reglamentas. Duomenų saugumo standartai numatomi rekomendacinio pobūdžio ES tinklų ir informacijos saugumo agentūros priimtuose šaltiniuose. BDAR nėra numatyta imperatyvių saugumo

⁷⁹ 1981 m. sausio 28 d. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) pakeista 2018 m. gegužės 18d. protokolu (CETS Nr. 223) [interaktyvus, žiūrėta 2019 m. rugsėjo 24 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872>>.

⁸⁰ 1980 m . Ekonominio bendradarbiavimo ir plėtros organizacijos privatumo gairės [interaktyvus, žiūrėta 2019 m. rugsėjo 15 d.]. Prieiga per internetą: <<http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>>.

⁸¹ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p.129.

priemonių sąrašo, todėl duomenų valdytojo ir tvarkytojo atsakomybė nurodoma taip pat negriežtais imperatyvais „, siekti užtikrinti, tiek, kiek reikia „,

Pavojumi asmenims grįsto požiūrio principas iš esmės reiškia, kad duomenų valdytojas ir tvarkytojas prioritetu privalo laikyti duomenų tvarkymo saugumą. Šis principas įpareigoja kiek tai įmanoma įvertinti galimus pavojus ir imtis tinkamų priemonių. Pagal BDAR 32 str. 2 d. „, Nustatant tinkamo lygio saugumą visų pirma atsižvelgiama į pavojus, kurie kyla dėl duomenų tvarkymo, visų pirma dėl netyčinio arba neteisėto persiųstų, saugomų ar kitaip tvarkomų duomenų sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų.“

Duomenų konfidencialumo, vientisumo, prieinamumo ir atsparumo principas – kitais žodžiais tariant laikomas saugumo užtikrinimo pagrindiniais kriterijais. Šio principo savitumas yra toks, kad duomenų saugumas turi būti ne trumpalaikis, ar tam tikru laikotarpiu, o nepertraukiamai pagal BDAR 32 str. b p. gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą. Prieinamumo principas numato saugumo užtikrinimą neteisėtam asmens duomenų sunaikinimui ar praradimui, vientisumo reikalavimu taikomos technologijos užtikrinti asmens duomenų nepakeitimą bei konfidencialumo principas draudžia neteisėtą asmens duomenų atskleidimą duomenų tvarkymo sistemoje ar prieigą prie jų neturint tam leidimo.⁸² Tačiau nepakanka vien tik numatyti tam tikrų priemonių dėl saugumo duomenų valdytojui ir tvarkytojui, turi būti atliekami reguliarūs tikrinimai dėl jų techninių ir organizacinių priemonių veiksmingumo pagal BDAR 32 str. 1 d. p.

Kaip jau buvo užsiminta saugumo užtikrinimui naudojamos techninės ir organizacinės priemonės, kurios nustatytos norminiu lygiu ir ne. BDAR kelias saugumo priemones: 32 str. 4 d. numato, kad duomenų valdytojas ir duomenų tvarkytojas imasi priemonių, siekdami užtikrinti, kad bet kuris duomenų valdytojui arba duomenų tvarkytojui pavaldus fizinis asmuo, galintis susipažinti su asmens duomenimis, jų netvarkytų, išskyrus atvejus, kai duomenų valdytojas duoda nurodymus juos tvarkyti, nebent tas asmuo privalo tai daryti pagal Sąjungos arba valstybės narės teisę; BDAR 32 str. 1 d. a p. pseudonimų suteikimą asmens duomenims ir jų šifravimą; BDAR 32 str. 1 d. c p. jei reikia, gebėti laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju. Kitas saugumo priemones galima išvesti, pvz.: duomenų saugumą padeda užtikrinti ta, kad organizacija tvarko duomenų tvarkymo veiklos įrašud (BDAR 30 str. 1 d.), atlieka poveikio

⁸² 2014 m. kovo 25 d. ES 29 str. darbo grupės nuomonė Nr.693/14 dėl pranešimo apie asmens duomenų saugumo pažeidimą, p.4 [interaktyvus, žiūrėta 2019 m. spalio 29 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf>.

duomenų apsaugai vertinimą (35 str. 1 d.) arba paskiria duomenų apsaugos pareigūną (BDAR 37 str. 1 d.).⁸³ Taip pat neužtenka vien remtis šiomis nuostatos duomenų tvarkytojui ir valdytojui, nes turi būti įgyvendintos visos tinkamos techninės ir organizacinės priemonės , kurių duomenų valdytojo ir tvarkytojo nuomone reikėtų imtis (BDAR 32 str. 1 d.).

Už techninių ir organizacinių priemonių netaikymą ir kitus neteisėtus duomenų valdytojo veiksmus tvarkant asmens duomenis - taikoma atsakomybė, kuri išvedama iš atskaitomybės principo. Šis principas BDAR naujovė, nes iki tol nebuvo aiškiai ir tiksliai išreiškiamas kaip toks. Pagal BDAR 5 str. 2 d. duomenų valdytojas privalo užtikrinti, kad būtų laikomasi visų duomenų apsaugos principų ir prireikus privalo tai sugebėti įrodyti. EBPO privatumo gairių 14 str. ir ET duomenų apsaugos konvencijos 10 str. numato panašias nuostatas kaip ir BDAR 5 str. 2 d.

Vykdamas duomenų tvarkymo operacijas gali kilti didelis pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas turėtų būti atsakingas už poveikio duomenų apsaugai vertinimo atlikimą, kad būtų įvertinta visų pirma to pavojaus kilmė, pobūdis, specifika ir rimtumas. Į šio vertinimo rezultatus turėtų būti atsižvelgta nustatant tinkamas priemones, kurių būtų imtasi siekiant įrodyti, kad asmens duomenų tvarkymas vykdomas laikantis BDAR. Kai iš poveikio duomenų apsaugai vertinimo paaiškėja, kad duomenų tvarkymo operacijos susijusios su dideliu pavojumi, kurio duomenų valdytojas negali sumažinti tinkamomis priemonėmis, atsižvelgiant į turimas technologijas ir įgyvendinimo sąnaudas, prieš pradėdamas duomenų tvarkymą turėtų būti konsultuojamasi su priežiūros institucija. (BDAR preambulės 84 p.) Šį principą sudaro du elementai : pirmasis apima reikalavimus organizacijose taikyti tinkamą vidaus politiką bei priemones, antrasis numato, kad duomenų valdytojais turi turėti vidinius mechanizmus, kad galėtų įrodyti atitiktį priežiūros institucijoms (suinteresuotiems asmenims).⁸⁴ Atskaitomybės principas aiškiai reikalauja, kad duomenų valdytojais įgyvendintų tinkamas ir veiksmingas priemones duomenų apsaugos teisės principams užtikrinti, ir paprašius turi gebėti tai įrodyti.⁸⁵

Šį principą detalizuojančios BDAR normos: BDAR 24 str. 1 d. Atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą bei tikslus, taip pat į įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas įgyvendina tinkamas technines ir organizacines priemones, kad užtikrintų ir galėtų įrodyti, kad

⁸³ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p.133.

⁸⁴ *Ibid.*, p.135.

⁸⁵ 2010 liepos 13 d. ES 29 str. darbo grupės nuomonė Nr. 3/2010 dėl atskaitomybės principo, p.4 [interaktyvus. Žiūrėta 2019 m. lapkričio 1 d.]. Prieiga per internetą: < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf>.

duomenys tvarkomi laikantis šio reglamento. Tos priemonės prireikus peržiūrimos ir atnaujinamos. BDAR 35 str. 1 d. dėl duomenų tvarkymo rūšies, visų pirma, kai naudojamos naujos technologijos, ir atsižvelgiant į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, fizinių asmenų teisėms bei laisvėms gali kilti didelis pavojus, duomenų valdytojas, prieš pradėdamas tvarkyti duomenis, atlieka numatytų duomenų tvarkymo operacijų poveikio asmens duomenų apsaugai vertinimą. Panašius didelius pavojus keliančių duomenų tvarkymo operacijų sekai išnagrinėti galima atlikti vieną vertinimą. BDAR 35 str. 7 d. d p. poveikio įvertinime pateikiama pavojams pašalinti numatytos priemonės, įskaitant apsaugos priemones, saugumo priemones ir mechanizmus, kuriais užtikrinama asmens duomenų apsauga ir įrodoma, kad laikomasi šio reglamento, atsižvelgiant į duomenų subjektų ir kitų susijusių asmenų teises ir teisėtus interesus. Neišvengiamai atskaitomybės principo užtikrinimui privalomas duomenų apsaugos pareigūnas, (BDAR 37 str. 1 d.) kuris turi būtų tinkamai ir laiku įtraukiamas į visų su asmens duomenų apsauga susijusių klausimų nagrinėjimą (BDAR 38 str. 1 d.). Duomenų valdytojai skatinami įgyvendinti duomenų apsaugos teisės reikalavimus ir tai įrodyti pagal duomenų apsaugos elgesio kodeksą (BDAR 40 str. 1 d.) ir duomenų apsaugos sertifikatai (BDAR 42 str. 1 d.)⁸⁶ Duomenų valdytojas šiuo principu įpareigojamas sugebėti įrodyti, kad tinkamai laikomasi asmens duomenų teisės. Šią pareigą detalizuojančios normos - BDAR 7 str. 1. Sugebėti įrodyti, kad duomenų subjektas davė sutikimo dėl asmens duomenų tvarkymo, BDAR preambulės 69 p. numato pareigą įrodyti, kad duomenų valdytojo interesas viršesnis už duomenų subjekto interesus, apie padarytą duomenų saugumo pažeidimą turi nedelsdamas pranešti kompetetingai institucijai per 72 valandas nebent sugebėtų įrodyti, kad nebuvo pavojaus fizinių asmenų teisėms (BDAR 33 str. 1 d.).

Socialiniuose tinkluose galima teigti, kad ne tik duomenų valdytojas atsako už duomenų saugumą. Dažnu atveju jauni žmonės, paaugliai siekdami populiarumo arba dėl neatsargumo dalinasi savo gyvenimu: kur gyvena, kokį automobilį vairuoja, kokiose prabangiose parduotuvėse lankosi. Pats socialinių tinklų vartotojas ypatingai susikūręs naują paskyrą ir neapribojęs privatumo nustatymais prieigos prie tokių duomenų, gali susidurti su paskyros „nulaužimu“ t.y. kuomet neteisėtu būdu naudojasi vartotojo paskyra kitas asmuo savo tikslais, tuo pačiu „nulaužiami“ ir elektroniniai paštai, kuriuose taip pat gausu asmeninės informacijos ir didelė rizika patirti ne tik teisės į privatumą pažeidimą, bet ir finansinių nuostolių, vagysčių bei kitų nusikalstamų veikų.⁸⁷ Todėl socialinių tinklų

⁸⁶ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p.136.

⁸⁷ HIATT D., B.CHOI Y. Role of Security in Social Networking (*IJACSA International Journal of Advanced Computer Science and Applications*, 2016, p.13).

vartotojai ypatingai nepilnamečiai, nesulaukę 16 m. privalo atsakingai ir apgalvotai dalintis asmenine informacija ir įvertinti visus galimus pavojus.

Taigi, duomenų atskaitomybės ir saugumo principai yra glaudžiai susiję, nes, jei nebus imtasi techninių ir organizacinių priemonių duomenų apsaugai užtikrinti arba bus parinktos nepakankamos, duomenų valdytojas turės pareigą tai įrodyti arba neįvertinęs galimo pavojaus asmenų teisėms ir laisvėms nepraneš kompetetingoms institucijoms, turės prisiimti atsakomybę už visas pasekmes kilusias duomenų subjektų teisėms. Tačiau socialinių tinklų vartotojai taip pat turi būti atsargūs ir apgalvotai privatumo nustatymuose apriboti prieigą siekiant apsaugoti nuo pašalinių asmenų „išsibrovimo“ į paskyrą, kad išvengtų nepageidaujamų nemalonumų.

3.6 Duomenų subjektų teisės ir duomenų apsaugos pareigūno vaidmuo

Socialiniai tinklai įpareigoti ne tik tinkamai tvarkyti asmens duomenis laikantis visų analizuotų asmens duomenų apsaugos principų, bet ir nepažeisti vartotojų – duomenų subjektų teisių. BDAR įtvirtina duomenų subjektų teises III skyriuje: teisė būti informuotam apie duomenų tvarkymą, teisė susipažinti su duomenimis ir juos ištaisyti, teisė į duomenų perkeliamumą, teisė nesutikti su duomenų tvarkymu, teisė apriboti duomenų tvarkymą, teisė būti pamirštam. Toliau bus bendrai aptariamos šios teisės atskleidžiant esmę bei duomenų pareigūno vaidmuo užtikrinant duomenų subjektų teises.

Teisė būti informuotam apie duomenų tvarkymą – ši teisė kyla iš jau analizuotų sąžiningumo ir skaidrumo principų. Svarbu pabrėžti, kad ši teisė nesusijusi su pareiga turėti teisėto duomenų tvarkymo pagrindą. Duomenų subjektui visais atvejais turi būti pranešama: apie duomenų valdytoją, tiksliau tariant apie jo tapatybę bei kontaktiniai duomenys pateikti (BDAR 13 str. 1 d. a p.), apie duomenų tvarkymo tikslus, kurie kaip nagrinėta ankstesniuose skyriuose, turi būti pateikti aiškiai, konkrečiai ir tokiu būdu bei forma, kad duomenų subjektas be jokių papildomų priemonių suprastų, kam yra tvarkomi jo duomenys (BDAR 13 str. 1 d. c p.), jei duomenys naudojami toliau bus kitu tikslu, taip pat privalo būti informuotas, taip pat turi būti pranešta apie duomenų saugojimo laikotarpį, jei nėra tikslaus, tai turi būti nurodyti kriterijai saugojimo laikotarpiui nustatyti (BDAR 13 str. 2 d. a p., 14 str. 2 d. a p.), teisę pateikti skundą priežiūros institucijai (BDAR 13 str. 2 d. d p.).

Teisė susipažinti su duomenimis ir juos ištaisyti - duomenų subjektas turi teisę iš duomenų valdytojo gauti patvirtinimą, ar su juo susiję asmens duomenys yra tvarkomi, o jei tokie asmens duomenys yra tvarkomi, turi teisę susipažinti su asmens duomenimis ir gauti informacijos apie jų tvarkymą (BDAR 15 str. 1 d.). Duomenų subjektui priskiriama teisė susipažinti su apie jį surinktais asmens duomenimis ir suteikiama galimybė per tam

tikrą laiką ja lengvai pasinaudoti, kad žinotų apie duomenų tvarkymą, galėtų patikrinti jo teisėtumą ir prireikus įgyvendinti kitas savo, kaip duomenų subjekto, teises.⁸⁸ Duomenų subjektas be išimties turi teisę gauti šią informaciją: patvirtinimą, kad duomenų valdytojas su duomenų subjektu susijusius duomenis (BDAR 15 str. 1 d), tvarkomus duomenis su duomenų kopija (BDAR 15 str. 1 d., 3 d.), duomenų tvarkymo tikslus (BDAR 15 str. 1 d. ap.), apie saugojimo terminus ar jų nustatymo kriterijus (BDAR 15 str. 1 d. c p.), susipažindamas su duomenimis ir pastebėjęs neatitikimų turi teisę ištaisyti duomenis (BDAR 16 str.).

Teisė į duomenų perkeliamumą – tik BDAR numatyta naujovė. Duomenų perkeliamumas yra teisė gauti duomenų valdytojo tvarkomus asmens duomenis ir laikyti juos tolesniam asmeniniam naudojimui privačiame įrenginyje, neperduodant jų kitam duomenų valdytojui. Šiuo atžvilgiu duomenų perkeliamumas papildo prieigos teisę. Duomenų perkeliamumo ypatumas yra tas, kad duomenų subjektams tai yra paprastas būdas patiems tvarkyti ir naudoti asmens duomenis taip juos kontroliuojant.⁸⁹ Teisei į duomenų perkeliamumą būdingi du elementai⁹⁰: pirma, duomenų subjektas turi teisę gauti duomenis, juos saugoti asmeniniame įrenginyje ir naudoti savo asmeniniams poreikiams. Antra duomenų subjektas turi teisę ne tik gauti ir pakartotinai naudoti duomenis, bet ir be kiūčių persiųsti savo pateiktus duomenis kitam paslaugų teikėjui, be to, turi teisę leisti vienam duomenų valdytojui tiesiogiai persiųsti asmens duomenis kitam, kai tai techniškai įmanoma (BDAR 20 str. 4 d.). Duomenų subjektas turi teisę gauti su juo susijusius asmens duomenis, kuriuos jis pateikė duomenų valdytojui susistemintu, įprastai naudojamu ir kompiuterio skaitomu formatu, tad ši teisė netaikoma popierinių bylų duomenims.

Teisė nesutikti su duomenų tvarkymu - duomenų subjektas turi teisę dėl su jo konkrečiu atveju susijusių priežasčių bet kuriuo metu nesutikti, kad su juo susiję asmens duomenys būtų tvarkomi išskyrus išimtis (BDAR 21 str. 1 d.). Teisė neleisti tvarkyti duomenų apima siekiant atlikti užduotį, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas, 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 (BDAR 6 str. 1 d. e

⁸⁸ Ibid, p. 171.

⁸⁹ 2016 m. gruodžio 13 d. ES 29 str. darbo grupės gairės dėl duomenų perkeliamumo nr. WP242, p.4 [interaktyvus, žiūrėta 2019 m. lapkričio 19 d.].

Prieiga per internetą: <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf>.

⁹⁰ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p.175.

ir f p.). Duomenų subjektų prieštaravimas duomenų tvarkymui reikalauja iš duomenų valdytojo palyginti su savo ir duomenų subjekto teises bei atitinkamus vienas kitam prieštaraujančius interesus, konkrečiau įvertinti visas su konkrečia duomenų subjekto padėtimi susijusias aplinkybes ir, kai prieštaraujama pagrįstai, toliau nebetvarkyti tokių duomenų⁹¹.

Teisė apriboti duomenų tvarkymą – teisė apriboti duomenų tvarkymą yra BDAR naujovė, kuri yra laikinoji duomenų subjekto apsaugos priemonė. Duomenų tvarkymo apribojimas reiškia saugomų asmens duomenų žymėjimą siekiant apriboti jų tvarkymą ateityje (BDAR 4 str. 3 p.). Kai duomenų tvarkymas yra apribotas, asmens duomenis galima tvarkyti, išskyrus saugojimą, tik gavus duomenų subjekto sutikimą arba siekiant pareikšti, vykdyti arba apginti teisinius reikalavimus, arba apsaugoti kito fizinio ar juridinio asmens teises, arba dėl svarbaus Sąjungos arba valstybės narės viešojo intereso priežasčių. Negalima atlikti jokių kitų duomenų tvarkymo veiksmų pvz.: rinkimo, įrašymo, rūšiavimo, sisteminimo ir pan. Apriboti galima duomenų naudojimą ir duomenų ištrynimą.⁹² Duomenų subjektas gali prašyti laikinai apriboti duomenų tvarkymą duomenų tikslumo užginčijimo pagrindu (BDAR 18 str. 1 d. a p.) arba prieštaravimo duomenų tvarkymui (BDAR 17 str. 1 d. d p.) Duomenų subjektas gali nesutikti su duomenų tvarkymu ir reikalauti jį apriboti, kai jis grindžiamas užduotimi, vykdoma dėl viešojo intereso ar duomenų valdytojui pavestų viešosios valdžios funkcijų arba trečiosios šalies interesų (BDAR 6 str. 1 d. e, f p.). Duomenų subjektas gali apriboti duomenų tvarkymą, kai duomenų valdytojui nereikia duomenų dėl numatytų tikslų, bet jų reikia dėl teisinių reiklavimų pateikimo ar vykdymo ir t.t.

Teisė būti pamirštam – tai teisė ištrinti duomenis. Šios duomenų subjekto teisės esmė yra reikalauti, kad duomenų valdytojas nepagrįstai nedelsdamas ištrintų su juo susijusius asmens duomenis, o duomenų valdytojas yra įpareigotas nepagrįstai nedelsdamas tai padaryti (BDAR 17 str. 1 d.). Duomenų subjektas turi teisę reikalauti, kad asmens duomenys būtų ištrinti ir nebenaudojami, kai šių duomenų nereikia nustatytiems tikslams, kuriais jie buvo renkami arba kitaip tvarkomi (BDAR 17 str. 1 d. a p.). Ištrinti būtina tokiu atveju, kai suėjo nustatyti duomenų saugojimo terminai (BDAR 5 str. 1 d. e p.). Taip pat teisė būti pamirštam turi būti įgyvendinama, kai duomenų subjektas atšaukė sutikimą tvarkyti jo duomenis ir tai buvo vienintelis duomenų tvarkymo pagrindas (BDAR 17 str. 1

⁹¹ ES Teisingumo teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*, 34 p. [interaktyvus, žiūrėta 2019 m. spalio 1 d.]. Prieiga per internetą: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=LT>>.

⁹² ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019, p.182.

d. b p.). Tačiau kaip ir visoms duomenų subjekto teisėms taikoma išimtis dėl viešojo intereso ir duomenų valdytojams pavestų viešosios valdžios funkcijų. Duomenų subjektas turi teisę prieštarauti tam, kad jo asmens duomenis indeksuotų paieškos variklis, jei dėl šių duomenų sklaidos per šį variklį jam sukeliama neigiami padariniai ir jei jo pagrindinės teisės į šių duomenų apsaugą ir į privataus gyvenimo gerbimą, kurios apima ir „teisę būti pamirštam“, yra viršesnės nei teisėti šio variklio eksploatuotojo interesai ir bendrasis informacijos laisvės interesas.⁹³ Tačiau taip nebūtų tuo atveju, kai dėl konkrečių aplinkybių, kaip antai šio subjekto padėties viešajame gyvenime, paaiškėtų, kad šių pagrindinių teisių apribojimą pateisina viršesnis šios visuomenės interesas turėti įtraukimo į atitinkamus sąrašus suteikiamą prieigą prie atitinkamos informacijos.⁹⁴ Kita svarbi teisė susijusi su socialiniuose tinkluose besinaudojančiais vaikais (ir ne tik), kuriems teisė būti pamirštam turi būti taikoma dėl tiesiogiai siūlomų informacinės visuomenės paslaugų (BDAR 17 str. 1 d. f p.). Ta teisė ypač svarbi tais atvejais, kai duomenų subjektas savo sutikimą išreiškė būdamas vaikas ir nevisiškai suvokdamas su duomenų tvarkymu susijusius pavojus, o vėliau nori, kad tokie – ypač internete saugomi – asmens duomenys būtų pašalinti. Duomenų subjektas turėtų galėti naudotis ta teise, nepaisant to, kad jis nebėra vaikas (BDAR preambulės 65 p.).

Užtikrinant duomenų subjektų teises iš šio viso darbo analizės aišku, kad duomenų valdytojui tenka pareiga įgyvendinti tiek duomenų subjektų teises, tiek taikyti visas būtinas organizacines ir technines priemones duomenų saugumui užtikrinti. Tačiau asmens duomenų apsauga nėra tik duomenų valdytojų pareiga, valstybės taikydamos BDAR taip pat privalo užtikrinti duomenų apsaugą, todėl paskiriami duomenų apsaugos pareigūnai. Tai nauja BDAR ypatybė pagal kurią duomenų apsaugos pareigūnas – darbuotojas ar išorės ekspertas (paslaugos tiekėjas), kuris prižiūri ir padeda užtikrinti duomenų valdytojo ir duomenų tvarkytojo atitiktį BDAR.⁹⁵ Duomenų apsaugos pareigūnas atlieka bent šias užduotis: informuoja duomenų valdytoją arba duomenų tvarkytoją ir duomenis tvarkančius darbuotojus apie jų prievoles pagal BDAR ir konsultuoja juos šiais klausimais; stebi, kaip laikomasi šio BDAR, kitų Sąjungos nacionalinės duomenų apsaugos nuostatų ir duomenų valdytojo arba duomenų tvarkytojo politikos asmens duomenų apsaugos srityje; paprašius konsultuoja dėl poveikio duomenų apsaugai vertinimo ir stebi jo atlikimą; bendradarbiauja su priežiūros institucija; atlieka kontaktinio asmens funkcijas priežiūros institucijai

⁹³ ES Teisingumo teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*, 91 p. [interaktyvus, žiūrėta 2019 m. spalio 1 d.]. Prieiga per internetą: <<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=LT>>.

⁹⁴ *Ibid.*, p.97.

⁹⁵ ZALESKIS, J. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017.

kreipiantis su duomenų tvarkymu susijusiais klausimais. Duomenų apsaugos pareigūnas, vykdydamas savo užduotis, tinkamai įvertina su duomenų tvarkymo operacijomis susijusį pavojų, atsižvelgdamas į duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus (BDAR 39 str.).

Taigi, duomenų subjektų teisių užtikrinimas yra pagrindinis BDAR tikslas, kurio pagalba užtikrinama apsauga ir socialiniuose tinkluose, tačiau už duomenų subjektų teisių įgyvendinimą atsako ne tik duomenų valdytojas, bet ir duomenų apsaugos pareigūnai, kurie prižiūri duomenų valdytojų ir tvarkytojų veiklą bei bendradarbiauja. Išanalizavus tiek teises, tiek pareigas numatytas duomenų subjektams ir duomenų valdytojams, toliau bus vertinama duomenų politiką socialiniame tinkle „Facebook“ ir bus nustatoma, ar tinkamai įgyvendinamas BDAR pagal išanalizuotą asmens duomenų apsaugos teisę.

4. ASMENS DUOMENŲ APSAUGOS TEISĖS PAŽEIDIMAI SOCIALINIUOSE TINKLUOSE

4.1 Duomenų politikos socialiniuose tinkluose „Facebook“ ir „Instagram“ vertinimas pagal BDAR reikalavimus

Šiame skyriuje bus nagrinėjama socialinių tinklų „Facebook“ ir „Instagram“ duomenų politika⁹⁶, kurių duomenų valdytojas yra bendrovė „Facebook Ireland“. Pagrindinis dėmesys analizuojant duomenų politiką bus kreipiamas į tikslo suformulavimą, duomenų tvarkymo teisėtumo pagrindus, ar galimai nepažeidžiami asmens duomenų apsaugos teisės principai išanalizuoti šiame darbe: teisėtumo, sąžiningumo ir skaidrumo, duomenų tvarkymo tikslo apribojimo, duomenų kiekio mažinimo, duomenų tikslumo.

Duomenų politikos aprašą „Facebook“ platformoje galima rasti per vartotojo profilį, konkrečiai paspaudus viršuje esantį „?“ mygtuką, o po jo „Privatumo nuorodos“ tada apačioje „ Teisinė informacija ir politikos nuostatos“ ir galiausiai „Duomenų politika“. Šioje skiltyje pateikiama bendro pobūdžio apie tvarkomus duomenis informacija, kaip teigia pats socialinis tinklas, o dėl „pasiekimo“ ir ištrynimo informacijos nukreipia į kitus nustatymus, kurie jau anglų kalba (prieš tai esanti bendra informacija pateikiama lietuvių kalba).

Pradėkime nuo pirmojo žingsnio prieš duomenų tvarkymą tai – aiškiai, nedviprasmiškai, tesėto tikslo suformulavimo analizės (BDAR 5 str. 1 d. b p.). Pastebėtina, kad aiškiai išskirtų tikslų kam panaudojami duomenis iš pirmo žvilgsnio sunku būtų surasti neperskaičius ir ne vieną kartą atidžiai visos duomenų politikos, tačiau randama galimai tikslus apibūdinanti informacija prie skilties „ Kaip naudojame šią informaciją“? Mano nuomone, žodis „ kaip“ apibūdina būdą, būtent kokiais būdais renkami asmens duomenys. Jei būtų patikslinta „Kam?“ ar „kokiems tikslams“, tuomet būtų visiškai tikslu ir aišku, jog šioje skiltyje pateikiama informacija apie asmens duomenų panaudojimo tikslus. Po pavadinimu nurodoma: „Turimą informaciją (atsižvelgiant į jūsų pasirinkimus) naudojame toliau aprašytais tikslais bei teikti ir palaikyti „Facebook“ produktus ir susijusias paslaugas, aprašytas „Facebook“ ir „Instagram“ sąlygose. Informaciją naudojame toliau nurodytais būdais.“ Šis sakinys iš pradžių nurodo, kad pateikiami tikslai, o po to būdai. Pagal BDAR minėtą straipsnį 5 str. 1 d. b p. tikslas turi būti aiškiai, suprantai, nedviprasmiškai išreiškštas, turi būti atskleistas lengvai suprantama forma ir nekelti jokių abejonių dėl turinio. Tikslų apibrėžimas visų pirma turi būti išreikštas taip, kad jį vienodai suprastų ne tik duomenų valdytojas (įskaitant visus susijusius darbuotojus) bet ir suinteresuotieji

⁹⁶ Duomenų politika [interaktyvus, žiūrėta 2019 m. spalio 31 d.]. Prieiga per internetą: <<https://lt.lt.facebook.com/help/instagram/155833707900388>>.

asmenys: duomenų subjektai, duomenų apsaugos institucijos, duomenų tvarkytojai,⁹⁷ todėl vienoje vietoje pateikta duomenų tvarkymo būdų bei tikslų informacija, nėra laikytina aiškia, nedviprasmiška tikslo atžvilgiu, nes vartotojas tikėtina negebėtų pasirinkti pats, kur nurodyti būdai, o kur tikslai be teisininko pagalbos ar kito specialisto, taigi, tai galima laikyti BDAR 5 str. 1 d. b p. pažeidimu. Žinant faktą, kad tikslai ir būdai pateikiami vienoje vietoje, toliau paanalizuokite, kokiems tikslams panaudojami socialinių tinklų „Facebook“ ir „Instagram“ asmenys duomenys. Duomenų politikoje paryškinti šie tikslai ir/ ar būdai (kaip nurodė pats duomenų valdytojas), todėl pabandyčiau išskirti duomenų tvarkymo tikslus ir įvertinti, tikslai: „Teikti, asmeniškai pritaikyti ir pagerinti Produktus; Teikti vertinimo, analizavimo ir kitas verslo paslaugas; Skatinti saugą, vientisumą ir saugumą; Bendrauti su jumis; Atlikti tyrimus ir kurti naujoves socialinei gerovei.“

Pirmasis tikslas „Teikti, asmeniškai pritaikyti ir pagerinti Produktus“ – duomenų valdytojo paaiškinamas kaip „Turimą informaciją naudojame teikdami savo Produktus, įskaitant asmeniškai pritaikytas funkcijas ir turinį (įskaitant jūsų naujienų sklaidos kanalą, „Instagram“ sklaidos kanalą, „Instagram“ istorijas ir reklamas), bei pasiūlymus (pavyzdžiui, grupių ar renginių, kurie jums gali būti įdomūs, arba temų, kurias galbūt norėsite sekti, pasiūlymus) mūsų Produktuose ir kitur. Siekdami sukurti asmeniškai pritaikytus, unikalius ir jums aktualius Produktus, naudojame informaciją apie jūsų ryšius, nuostatas, pomėgius ir veiklą, pagrįstą duomenimis, kuriuos renkame ir sužinome iš jūsų ir kitų žmonių (įskaitant visus jūsų pateiktus duomenis, kuriems taikoma speciali apsauga, pasirenkate pateikti ten, kur davėte aiškų sutikimą); informaciją apie tai, kaip naudojate mūsų Produktus ir su jais sąveikaujate; ir informaciją apie žmones, vietas ar dalykus, prie kurių esate prisijungę ir kuriais domitės naudodami mūsų Produktus ir kitur. Sužinokite daugiau apie tai, kaip naudojame informaciją apie jus, siekdami pritaikyti „Facebook“ ir „Instagram“ jums asmeniškai, įskaitant funkcijas, turinį ir „Facebook“ Produktų rekomendacijas, taip pat apie tai, kaip parenkame jūsų matomas reklamas.“ Pastebima, kad tikslas suformuluotas gana neaiškiai, tačiau skaitant toliau galima suprasti, kad šiuo tikslu duomenų valdytojas leidžia rinkti „visą“ informaciją apie socialinių tinklų vartotoją, t.y informaciją apie vartotojų ryšius, nuostatas, pomėgius ir veiklą, pagrįstą duomenimis, kuriuos renka ir sužino iš varotojo ir kitų žmonių (įskaitant visus jūsų pateiktus duomenis, kuriems taikoma speciali apsauga, pasirenkate pateikti ten, kur davėte aiškų sutikimą); informaciją apie tai, kaip naudojami Produktai; ir informaciją apie žmones, vietas ar

⁹⁷2013 m. balandžio 2 d. ES 29 str. darbo grupės nuomonė Nr. 03/2013 dėl tikslo apribojimo Nr. WP203 [interaktyvus. žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.

dalykus, prie kurių esate prisijungę ir kuriais domitės naudodami mūsų Produktus ir kitur. Mano manymu, šis nurodytas tikslas įvardintas galimai neteisingai, nes iš esmės renkami duomenys nėra tik pagerinti siūlomus „Facebook“ produktus kaip „Messenger“ ir „Instagram“ ir jo funkcijas pašalinant trikdžius, bet ir naudojami asmens duomenys rinkodarai. Todėl šis tikslas rodo, jog galimai naudojami pertekliniai duomenys, tokiu atveju darytina išvada, kad galimai pažeidžiamas BDAR 5 str. 1 d. c p. duomenų kiekio mažinimo principas, nes nėra naudojami asmens duomenys tinkami ir tik tokie, kurių reikia siekiant tikslo, dėl kurių jie tvarkomi bei tokiu atveju pažeidžiama duomenų subjektų teisė dėl sutikimo pagal BDAR 7 str., nes tikėtina atskiro sutikimo rinkodarai leisti panaudoti asmens duomenis duomenų valdytojas nepateikia duomenų subjektui pagal šios duomenų politikos aprašymą tuo pačiu galimai pažeidžiami teisėtumo, sąžiningumo ir skaidrumo principai pagal BDAR 5 str. 1 d. a p.

Antrasis tikslas įvardintas „Teikti vertinimo, analizavimo ir kitas verslo paslaugas“ – „Turimą informaciją (įskaitant duomenis apie jūsų veiklą ne mūsų Produktuose, pavyzdžiui, lankomas svetaines ir matomas reklamas) naudojame tam, kad reklamuotojams ir kitiems partneriams padėtume įvertinti jų reklamų ir paslaugų efektyvumą ir pasiskirstymą bei suprasti, kokio tipo žmonės naudojami paslaugomis ir kaip žmonės sąveikauja su jų svetainėmis, programėlėmis ir paslaugomis. Sužinokite, kaip bendriname informaciją su šiais partneriais.“ Kadangi iš šio aprašymo tikslo nėra aišku, kas vertina, analizuoja ir teikia verslo paslaugas (kokios bendrovės įmonės ir pan), todėl toliau apie kiekvieną iš tikslu įvardintų sąvokų: apie vertinimą, analizavimą ir verslo paslaugas duomenų valdytojas paaiškina nuorofoje prieš tai pateiktame tikslo aprašyme, nuorofo: „sužinokite, kaip bendriname informaciją“. Vertinimas ir analizė „Vertinimo.partneriai.Informaciją apie jus bendriname su bendrovėmis, kurios ją apibendrina ir teikia analizės bei matavimo ataskaitas mūsų partneriams.“ Iš šio apibūdinimo, mano nuomone tik aišku, kad bendrina informaciją su bendrovėmis (kokiomis bendrovėmis konkrečiai nenurodyta) ir pateikia matavimo ataskaitas (neaišku, kas yra matavimo) partneriams (neįvardinti konkrečiai, kokie partneriai). Verslo partneriai – „Pardavėjai ir paslaugų teikėjai.Teikiame informaciją ir turinį pardavėjams ir paslaugų teikėjams, kurie padeda mūsų verslui, pavyzdžiui, teikia techninės infrastruktūros paslaugas, analizuoja, kaip naudojami mūsų Produktai, teikia klientų aptarnavimo paslaugas, sudaro palankesnes sąlygas atlikti mokėjimus ar atlieka apklausas.“ Taigi, vėl neaišku, kokiems konkrečiai verslo partneriams duomenų subjektų asmens duomenys panaudojami, nes neįvardinami pardavėjai, paslaugų teikėjai ir pan. Duomenų panaudojimo tikslai ir teisinis pagrindas bei asmens duomenų tvarkymas turėtų būti aiškus. Pvz.: Šios

frazės nėra pakankamai aiškios tvarkymo tikslams: „Mes galime naudoti jūsų asmens duomenis kurdami naujas paslaugas“ (nes neaišku, ką paslaugos yra ar kaip duomenys padės jas plėtoti); „Mes galime naudoti jūsų asmeninius duomenis tyrimų tikslais (nes neaišku kokie tyrimų tai reiškia); ir „Mes galime naudoti jūsų asmens duomenis siūlydami individualizuotas paslaugas“ (nes neaišku ką reiškia personalizavimas)⁹⁸. Todėl šis tikslas galimai pažeidžia skaidrumo principą (BDAR 5 str. 1 d. a p.), nes duomenų valdytojas galimai netinkamai atliko savo pareigą duomenų subjektui pateikti glausta, skaidria, suprantama ir lengvai prieinama forma, aiškia ir paprasta kalba dėl to, kad numatytas tikslas nukreipė į kitą nuorodą, kurioje irgi reikėjo man kaip vartotojui bandyti atsirinkti, kas ką apibūdina, nors taip neturėtų būti, nes pateikta turi būti kaip minėta glausta ir lengvai suprantama forma bei verslo partneriai, įmonės ir bendrovės, reklamuotojai nėra įvardijami konkrečiai, o tik bendriniais pavadinimais, kas taip pat galimai neatitinka šio principo.

Trečias tikslas - skatinti saugą, vientisumą ir saugumą. Po pavadinimu esantis aprašymas: „Turimą informaciją naudojame siekdami tikrinti paskyras ir veiklą, kovoti su žalingu elgesiu, išvengti šlamšto ir kito blogo turinio bei jį aptikti, išlaikyti Produktų vientisumą ir skatinti saugą bei saugumą „Facebook“ produktuose ir kitur. Pavyzdžiui, turimus duomenis naudojame siekdami tirti įtartą veiklą arba sąlygų ir politikos pažeidimus, arba nustatyti atvejus, kai kokiam nors žmogui reikalinga pagalba. Norėdami daugiau sužinoti, apsilankykite „Facebook“ saugumo pagalbos centre ir „Instagram“ saugumo patarimų skiltyje.“ Iš esmės tikslas suformuluotas ganai aiškiai, nedviprasmiškai ir tiksliai, jei skaitoma turint mintyje asmens duomenų apsaugą, tačiau pabrėžtina, kad tikslas tai ne tik mintys, bet ir aiškiai išreiškštas suprantama forma pagal tikslo apribojimo principą (BDAR 5 str. 1d. b p.), todėl vertėtų patikslinti kieno saugumas ir sauga, tačiau kita vertus po pavadinimu esančiame aprašyme konkretizuojama keliais pavyzdžiais, kokiam saugumui renkami asmens duomenys t.y. kovai su žalingu elgesiu (konkretizuoti vertėtų), išvengti šlamšto (konkretizuoti vertėtų, nes neaišku, kas yra šlamštas) ir kito blogo turinio (neaišku, kas yra blogas turinys, konkretizuoti), skatinti saugumą „Facebook“ ir jo produktuose. Nurodyta nuoroda nukreipia konkrečiai kaip apsaugoti savo asmeninį vartotojo profilį t.y. slaptažodį, savo profilį, kokias saugumo priemones galima naudoti, bet visa informacija pateikiama jau užsienio kalba t.y. – anglų kalba, kas taip pat gali pažeisti minėtąjį skaidrumo principą, nes ne visi Facebook vartotojai gali suprasti šią užsienio ir

⁹⁸ 2017 m. ES 29 str. darbo grupės gairės dėl skaidrumo [interaktyvus, žiūrėta 2019 m. spalio 18 d.]. Prieiga per internetą: <https://iapp.org/media/pdf/resource_center/wp29-transparency-12-12-17.pdf>.

nebeatitiktų „lengvai, aiškiai suprantamai“ pateiktos duomenų subjektui formos bei pats tikslas taip pat suformuluotas galimai neaiškiai.

Ketvirtasis tikslas - Bendrauti su jumis. „Turimą informaciją naudojame, kad siųstume jums rinkodaros pranešimus, bendrautume su jumis dėl mūsų Produktų ir praneštume apie mūsų politiką ir sąlygas. Jūsų informaciją taip pat naudojame, kad atsakytume, kai į mus kreipiatės.“ Na, tokio tikslo, mano manymu, nelabai tikslinga vadinti savarankišku tikslu, nes įterpiama tiesioginė rinkodara ir socialinio tinklo politika bei sąlygos, kas jau kaip buvo analizuota ankstesniame pirmame tikslu turi būti atskiras tikslas su duomenų subjektų pateiktu sutikimu dėl tiesioginės rinkodaros. Todėl galimai pažeidžia duomenų tvarkymo tikslo apribojimo principą, skaidrumo, teisėtumo ir sąžiningumo principus (BDAR 5 str.) bei galimai duomenų subjekto sutikimo nebuvimo tiesioginės rinkodaros aspektu.

Penktas tikslas - atlikti tyrimus ir kurti naujoves socialinei gerovei. „Turimą informaciją (įskaitant informaciją, gautą iš tyrimų partnerių, su kuriais bendradarbiaujame) naudojame siekdami atlikti ir remti tyrimus bei naujoves, susijusius su bendrąja socialine gerove, technologine pažanga, viešaisiais interesais, sveikata ir gerove. Pavyzdžiui, analizuojame turimą informaciją apie migracijos modelius per krizes, kad padėtume teikti pagalbą. Sužinokite daugiau apie mūsų tyrimų programas.“ Pats tikslas suformuluotas ganai aiškiai iš pirmo žvilgsnio, nes jį papildoma apačioje esantis aprašymas, kad asmens duomenys panaudojami viešajam interesui užtikrinti, technologiniais tyrimų tikslais galimai (technologine pažanga), tačiau duomenų valdytojui vertėtų žinoti, kad dažnai būna neįmanoma asmens duomenų rinkimo metu galutinai nustatyti, kad duomenys bus tvarkomi mokslinių tyrimų tikslais. Todėl duomenų subjektai turėtų turėti galimybę duoti sutikimą dėl tam tikrų mokslinių tyrimų sričių, laikantis pripažintų mokslinių tyrimų srities etikos standartų. Duomenų subjektai turėtų turėti galimybę duoti sutikimą tik dėl tam tikrų tyrimų sričių arba tyrimų projektų dalių tiek, kiek tai leidžiama pagal numatytą tikslą (BDAR preambulės 33 p.) bei nėra aišku kokie duomenys naudojami sveikatos gerovei bei kokie partneriai su kuriais bendradarbiaujama (konkrečiai neįvardinta), kokie tie tyrimai iš partnerių ir kas tie partneriai, todėl išanalizavus šį tikslą sunku būtų teigti, kad jis yra visiškai tikslus ir teisingas bei pateikiamos nuorodos dėl migracijos modelių per krizes bei apie tyrimų programos vėl užsienio kalba, kas irgi nėra skaidru, teisinga ir sąžininga BDAR atžvilgiu.

Dėl teisinių pagrindų tvarkant asmens duomenis - duomenų politikoje numatyti duomenų tvarkymo pagrindai: „kiek tai būtina vykdyti „Facebook“ paslaugų sąlygas arba „Instagram“ paslaugų sąlygas; su jūsų sutikimu, kurį bet kada galite atšaukti „Facebook“ ir „Instagram“ nustatymuose; kiek tai būtina laikytis mūsų teisinių

prievolių; apsaugoti gyvybinius jūsų ir kitų interesus; kiek tai būtina užtikrinti viešuosius interesus; ir kiek tai būtina mūsų (ar kitų) teisėtiems interesams, įskaitant mūsų interesą teikti naujoviškas, asmeniškai pritaikytas, saugias ir pelningas paslaugas savo naudotojams ir partneriams, užtikrinti, išskyrus atvejus, kai už šiuos interesus yra viršesni jūsų interesai ar pagrindinės teisės ir laisvės, dėl kurių reikia apsaugoti asmens duomenis. Išsamesnė informacija pateikiama nuorodoje „sužinoti daugiau“. Duomenų tvarkymas turėtų būti teisėtas ir sąžiningas. Taikant skaidrumo principą, fiziniams asmenims turėtų būti aišku, kaip su jais susiję asmens duomenys yra renkami, naudojami, su jais susipažįstama arba jie yra kitaip tvarkomi, taip pat kokiu mastu tie asmens duomenys yra ar bus tvarkomi. Pagal skaidrumo principą informacija ir pranešimai, susiję su tų asmens duomenų tvarkymu, turi būti lengvai prieinami ir suprantami, pateikiami aiškia ir paprasta kalba. Tas 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 teise gauti patvirtinimą dėl su jais susijusių asmens duomenų tvarkymo ir teise 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. Visų pirma konkretūs tikslai, kuriais tvarkomi asmens duomenys, turėtų būti aiškūs, teisėti ir nustatyti duomenų rinkimo metu. Asmens duomenys turėtų būti tinkami, susiję su tikslais, kuriais jie tvarkomi, ir riboti pagal tai, kiek jų yra būtina turėti atsižvelgiant į tikslus, kuriais jie tvarkomi; tam pirmiausia reikia užtikrinti, kad asmens duomenų saugojimo laikotarpis būtų tikrai minimalus. Asmens duomenys turėtų būti tvarkomi tik tuomet, jei asmens duomenų tvarkymo tikslo pagrįstai negalima pasiekti kitomis priemonėmis. Siekiant užtikrinti, kad duomenys nebūtų laikomi ilgiau nei būtina, duomenų valdytojas turėtų nustatyti duomenų ištrynimo arba periodinės peržiūros terminus. Reikėtų imtis visų pagrįstų priemonių, siekiant užtikrinti, kad netikslūs asmens duomenys būtų ištaisyti arba ištrinti. Asmens duomenys turėtų būti tvarkomi taip, kad būtų užtikrintas tinkamas asmens duomenų saugumas ir konfidencialumas, be kita ko, užkertant kelią neteisėtai prieigai prie asmens duomenų ir jų tvarkymui skirtos įrangos ar neteisėtam jų naudojimui; kad duomenų tvarkymas būtų teisėtas, asmens duomenys turėtų būti tvarkomi gavus atitinkamo duomenų subjekto sutikimą arba remiantis kitu teisėtu pagrindu. (BDAR preambulės 39-40 p.). Taigi, nuorodoje plačiau, kaip nurodė duomenų valdytojas, įvardina, kokius duomenis renka duomenų subjekto sutikimu: „duomenims, kuriems taikoma speciali apsauga, tvarkyti (pvz., jūsų religinės pažiūros, politinės pažiūros, pomėgiai ar jūsų sveikata, jei šią informaciją bendrinate savo „Facebook“ profilio laukuose

arba skiltyje „Gyvenimo įvykiai“), kad galėtume bendrinti su jūsų pasirinktais asmenimis ir asmeniškai pritaikyti turinį. Veido atpažinimo technologijai naudoti. Duomenims, kuriuos apie jūsų veiklą nesinaudojant „Facebook“ įmonės produktais mums pateikia reklamuotojai ir kiti partneriai, tvarkyti, kad galėtume asmeniškai pritaikyti reklamas, rodomas jums „Facebook“ įmonės produktuose, svetainėse, programėlėse ir įrenginiuose, kuriuose naudojamos mūsų reklamos paslaugos. Jus identifikuojantiems duomenims (tokios informacijos kaip jūsų vardas ar el. pašto adresas, kuri gali būti naudojama su jumis susisiekti ar jus identifikuoti) bendrinti su reklamuotojais, pvz., kai nukreipiate mus, kad bendrintume jūsų kontaktinę informaciją su reklamuotoju, kad jis galėtų su jumis susisiekti, pavyzdžiui, norėdamas suteikti papildomos informacijos apie reklamuojamą produktą ar paslaugą. Informacijai, kurią mums leidžiate gauti per jūsų įjungtus įrenginio nustatymus (pvz., prieigos prie GPS vietos, fotoaparato ar nuotraukų) rinkti, kad galėtume teikti funkcijas ir paslaugas, apibūdinamas jums įjungus šiuos nustatymus.“ Taip pat nurodo sutikimo atsisakymo teisę bet kuriuo metu „Facebook“ ir „Instagram“ nustatymuose. Iš esmės, sutikimo duomenų tvarkymo teisiniai pagrindai nurodyti gana aiškiai, suprantamai ir konkrečiai, kam reikia sutikimo, tačiau, analizuojant iškilo klausimas, ar pateikiamas vienas sutikimas „viskam“, kas nurodyta, ar kiekvienam asmens duomenų panaudojimui, t.y. teisėtam duomenų tvarkymui, kurie minėti, atskirai. Bei pastebėtina, kad tiesioginė rinkodara yra priskirta ne prie sutikimo kaip vieno iš teisėto tvarkymo pagrindų, o pateikiama kaip atskiras teisėtas interesas. Tačiau norint tiesioginė rinkodara laikyti teisėtu interesu, privalu atsižvelgti į specialųjį šią sritį reglamentuojantį, teisės normų konkurencijos atveju pirmenybę prieš BDAR turintį elektroninių ryšių reguliavimą.⁹⁹ Pavyzdžiui, Lietuvoje pagal Elektroninių ryšių įstatymo 69 str. 1 d. naudoti elektroninių ryšių paslaugas, įskaitant elektroninio pašto pranešimų siuntimą, tiesioginės rinkodaros tikslu leidžiama tik gavus išankstinį abonentu ar registruoto elektroninių ryšių paslaugų naudotojo sutikimą. Pagal BDAR 21 str. duomenų subjektas turi teisę bet kuriuo metu nesutikti, jei su juo susiję asmens duomenys tvarkomi tiesioginės rinkodaros tikslais. Dėl duomenų nesutikimo pateikimo, buvo pabandyta susirasti „Facebook“ nustatymuose (kad būtų aiškiau, pateiksiu visų žingsnių eigą beišskant sutikimo atsisakymo pateikimo). Visų pirma, ši galimybė nurodyta duomenų politikoje „Kaip galite įgyvendinti BDAR jums suteiktas teises?“, kur pateikiama aktyvi nuoroda „teisė nesutikti“, ją paspaudus matomas jau anglų kalba pateikiamas „Managing your data & submitting objections“ informacinis langas, kur angliškai apačioje nurodoma, kuri socialinį tinklą dėl duomenų tvarkymo

⁹⁹ ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registru centras, 2019, p.160-161.

norima tvarkyti: „Facebook“ ir „Instagram“. Atlikus kelis paspaudimus tk tuomet galima pateikti atsisakymą nurodant pačiam duomenų subjektui. Ar toks pateikimas atitinka BDAR sąžiningumo, skaidrumo ir teisėtumo principus, kurie užtikrina suprantama kalba ir forma bei aiškiu turiniu pateikiamą informaciją, tai klausimas ir galimai toks duomenų sutikimo pateikimas nėra visiškai teisėtas ir teisingas duomenų subjektų teisių atžvilgiu. Kiti nurodyti teisėti duomenų tvarkymo pagrindai kaip ir atitinkantys BDAR, tačiau šis „Atlikti tyrimus ir kurti naujoves socialinei gerovei. Teisėtas interesas, kuriuo remiamės taip tvarkydami duomenis, yra nurodytas toliau. Prisidėti prie pažangaus ar akademinio svarbių socialinių aspektų suvokimo, kad visuomenei ir pasauliui galėtume daryti teigiamą poveikį.“ Nėra aišku, kas yra pažangus ir svarbus socialinių aspektų suvokimas bei visuomenei ir pasauliui daromas poveikis, iš tokio teisėto intereso sunku suprasi, kokie gali būti galimai renkami duomenų subjekto duomenys.

Taigi, įvertinus duomenų politiką pagal BDAR pagrindinius reikalavimus keliamus duomenų valdytojui dėl tikslo suformulavimo, duomenų tvarkymo teisėtų pagrindų ir duomenų subjekto teisės – sutikimo, pabrėžtina, kad tikslai galimai nėra suformuluoti ir pateikiami aiškia, suprantama ir aiškaus turinio, nes tiesioginės rinkodaros tikslas nėra suformuluotas kaip toks, kaip savarankiškas, o implikuotas su kitais bei patys tikslai reikalauja aiškumo, o ne įvardinimo abstrakčiais žodžiais kaip bus tvarkomi asmens duomenys, vertinant duomenų tvarkymo teisėtumo pagrindus iš esmės dauguma jų teisėti, bet yra vienas neaiškus ir neleidžiantis suprasti, kokie duomenys bus panaudojami dėl socialinės gerovės ir pasauliui daromo teigiamo poveikio bei pažymėtina, kad duomenų valdytojas pateikia duomenų sutikimo ir tuo pačiu atsisakymo galimybę dėl duomenų tvarkymo, tačiau ji įgyvendinta galimai netinkamai, nes pateikiama užsienio kalba, kas galimai pažeistų skaidrumo, sąžiningumo ir teisėtumo principus. Kadangi rasta galimai pažeidimų, svarbu įvertinti, kokia teismų praktika ir kokie nustatyti pažeidimai asmens duomenų apsaugoje socialiniuose tinkluose.

4.2 Asmens duomenų teisės pažeidimai socialiniuose tinkluose naujausioje teismų praktikoje

Magistro darbe analizuota dėl asmens duomenų ir privatumo santykio, kuriuo paaiškinta, kad nesvarbu, jei socialiniame tinkle esi viešas visuomenėje asmuo, ar viešas profilis (visiems vartotojams prieinamas) privačių duomenų apie asmenį savais tikslais negalima naudoti. Viena iš reikšmingų bylų yra Lietuvos Respublikos vyriausiojo teismo byla dėl socialiniame tinkle „Facebook“ skelbiamų duomenų bei jų panaudojimo mokumo

vertinimui.¹⁰⁰ UAB „Creditinfo“ yra formuojama fizinių ir juridinių asmenų kredito istorija, nustatomi kredito reitingai bei asmenų galimybės prisiimti finansinius įsipareigojimus. Kredito biurą administruojanti UAB „Creditinfo Lietuva“ valdo gyventojams skirtą kredito istorijos sistemą „Mano Creditinfo“. Bendrovė nusprendė sudaryti galimybes fiziniams asmenims savitarnos svetainėje www.manocreditinfo.lt sužinoti savo kredito reitingą, kuris apskaičiuojamas iš socialiniuose tinkluose esančios informacijos (šiuo atveju iš „Facebook“ socialinio tinklo). Toks tikslas ir duomenų tvarkymas yra neteisėti. Teismas pabrėžė, jog asmens duomenys gali būti tvarkomi tik esant apibrėžtiems ir teisėtiems tikslams, turi sutapti duomenų paskelbimo ir tvarkymo tikslai, turi būti užtikrintas asmens privataus gyvenimo neliečiamumas, asmens susirašinėjimas, pokalbiai telefonu, bendravimas socialiniuose tinkluose. Teismas rėmėsi Lietuvos Respublikos Konstitucijos (toliau – ir Konstitucija) 22 straipsniu, Visuotinės žmogaus teisių deklaracijos (toliau – ir Deklaracija) 12 straipsniu, Žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos (toliau – ir Konvencija) 8 straipsniu. Pažymėjo, jog Europos Žmogaus Teisių Teismas (toliau – ir EŽTT) savo sprendimuose ne kartą yra pabrėžęs, kokia informacija ir kokiais būdais renkama, net ir viešame kontekste, gali patekti į asmens privataus gyvenimo sferą. EŽTT 1992 m. gruodžio 16 d. sprendime byloje *Niemietz prieš Vokietiją* konstatavo, kad nėra nei galimybės, nei būtinybės pateikti išsamią (baigtinę) „privataus gyvenimo“ sąvokos apibrėžtį; kad būtų per daug siaura šią sąvoką apriboti „artimiausia asmens aplinka“, kurioje asmuo gali savo nuožiūra gyventi savo asmeninį gyvenimą, visiškai pašalinant iš šios sąvokos išorinį pasaulį, kurio ši aplinka neapima. EŽTT 2004 m. birželio 24 d. sprendime *Von Hannover prieš Vokietiją* dar kartą pažymėjo esminę privataus gyvenimo apsaugos svarbą kiekvieno žmogaus asmenybės raidos požiūriu ir konstatavo, kad ši apsauga apima ne tik privačią šeimos, bet ir socialinę erdvę, kad kiekvienas asmuo (net jei jis ir yra žinomas plačiajai visuomenei) turi turėti galimybę naudotis teise į teisėtą lūkestį dėl savo privataus gyvenimo apsaugos ir gerbimo. Tokie duomenų subjekto socialinio tinklo profilio „Facebook“ duomenys kaip draugų sąrašas, kvietimai draugauti, draugų santykiai, socialiniame tinkle atskleista privati informacija (asmens kilmė, politiniai, religiniai ar kiti įsitikinimai, sveikata, lytinis gyvenimas, teistumas ar pan.), savaime preziumuoja, kad bus renkami tam tikri trečiųjų asmenų duomenys, kurie sutikimo nedavė, šie asmenys apie tokį duomenų tvarkymą net nesužinos, nes informacija apie

¹⁰⁰ Lietuvos Vyriausiojo administracinio teismo teisėjų kolegija. 2016 m. birželio 13 d. nutartis administracinėje byloje UAB „Creditinfo Lietuva“ v. Valstybinė duomenų inspekcija, Nr. A-408-858/2016.

atliktus asmens duomenų tvarkymo veiksmus ir nustatytą reitingą bus pateikiama tik asmeniui, kuris pageidavo tokį reitingą gauti. Atitinkamai, pareiškėjo nurodymas, kad sutikimas buvo surašytas „Facebook“ naudojamais terminais, šio socialinio tinklo vartotojams jie gerai žinomi, aktyviai naudojami, dar nereiškia, kad sutikimas yra aiškus ir suprantamas, apsisprendžiant dėl asmens duomenų tvarkymo mokumo vertinimo tikslu. Teismas laikė, kad pareiškėjo pateiktas sutikimo dėl duomenų tvarkymo tekstas nėra suprantamas ir aiškus, yra surašytas ne valstybine kalba, įterpiančią keletą lietuviškų žodžių, tekste nėra tiksliai nurodyta duomenų tvarkymo apimtis ir padariniai. Atitinkamai, teismas sprendė, jog pareiškėjo noras rinkti, tvarkyti, naudoti duomenis apie asmenį iš socialinių tinklų (konkrečiai „Facebook“), vertinant klientų mokumą ar sudarant kredito reitingą, prieštarauja teisėtam duomenų tvarkymui, neatitinka nustatytų reikalavimų, neužtikrina asmens privataus gyvenimo neliečiamumo (asmens susirašinėjimo, bendravimo socialiniuose tinkluose privatumo).

Kita byla¹⁰¹ susijusi su šiame darbe analizuota duomenų politika, konkrečiai su „Facebook“ pateikiamais duomenų tvarkymo tikslais. „Facebook“ su kitomis bendrovėmis, kurių viena įsteigta Jungtinėje Karalystėje neteisėtai tvarkė asmens duomenis ir paskirta 500000 svarų sterlingų bauda. Nuo 2013 m. lapkričio mėn. iki 2015 m. gruodžio mėn. „Facebook UK“ teikė tam tikras paslaugas „Facebook Ireland Limited“ kaip paslaugų teikėja ir duomenų valdytoja „Facebook“ paslaugas vartotojams ES, įskaitant Jungtinę Karalystę „Facebook UK“ teikiamos paslaugos apėmė rinkodaros ir reklamos palaikymą tam tikriems didesniems reklamuotojams, norintiems reklamuotis „Facebook“ platformoje. „Facebook“ įmonės tvarkė asmens duomenis įsteigtoje „Facebook UK“ bendrovėje. Jungtinės Karalystės (toliau JK) vartotojai apimtų JK gyventojus, kurie faktinių aplinkybių metu naudojo „Facebook“ svetainę (bet tuo neapsiriboja). JK vartotojai taip pat apimtų asmenis, besilankančius JK, kurie faktinių aplinkybių metu, lankydami JK, pasinaudojo „Facebook“ svetaine. Kadangi „Facebook“ įmonės tvarkė asmens duomenis apie JK vartotojus „Facebook UK“ bendrovės įsteigimo kontekste, todėl „Facebook“ įmonės nesąžiningai tvarkė asmens duomenis ir „Facebook“ įmonės nesiėmė tinkamų techninių ir organizacinių priemonių prieš neteisėtą asmens duomenų tvarkymą. Ginčas kilo dėl to, kad buvo naudojama programa (angl. app), kuri nebuvo suderinta su socialinio tinklo duomenų politika, t.y. asmens duomenys apie vartotojus buvo renkami be jų informavimo ir jų laisva valia aiškiai išreikšto sutikimo, nors bendrovė „Facebook“ prisipažino, kad remiantis

¹⁰¹ 2018 m. spalio 24 d. Facebook Ireland Ltd penalty notice [interaktyvus, žiūrėta 2019 m. lapkričio 6 d.]. Prieiga per internetą: < <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>>.

platformos politikos 3.3 skyriumi, gauti duomenys apie programos vartotojų draugus turėjo būti naudojami tik patobulinti tų naudotojų patirtį programoje, tačiau iš tikrųjų asmens duomenys buvo parduoti trečiosioms šalims. Be to, 2014 m. bendrovė įsipareigojo, kad programa bus naudojama tik mokslinių tyrimų, o ne komerciniais tikslais. „Facebook“ įmonės nesiėmė jokių veiksmų arba nepakankamai ėmėsi priemonių, kad užtikrintų, jog programa vykdoma nuosekliai su įmone. Svarbu pabrėžti, kad prieiga prie programos buvo nutraukta tik tada, kai buvo paskelbta „Guardian“ laikraštyje. „Facebook“ bendrovės nesąžiningai apdorojo „Facebook“ svetainės vartotojų asmeninius duomenis, įskaitant: tuos, kurie buvo Programos vartotojai; tie, kurie apsikeitė „Facebook“ žinutėmis su programos vartotojais; ir tie, kurie buvo „Facebook“ draugai su programos vartotojais. Facebook“ įmonės leido programai veikti taip, kad ji rinko asmens duomenis apie programos vartotojų „Facebook“ draugus, be to, „Facebook“ draugai nebuvo informuojami apie tai, kad tokie duomenys renkami bei neprašant jų sutikimo. „Facebook“ įmonės nebandė sutrukdyti programai tokiu būdu rinkti duomenis; pavyzdžiui, tokio duomenų rinkimo forma nebuvo uždrausta platformos politikoje. Leisdami programai veikti tokiu būdu, "Facebook" bendrovės nesąžiningai apdorojo programos vartotojų „Facebook“ asmeninius duomenis. „Facebook“ įmonės nesiėmė jokių priemonių apsisaugoti nuo tokio neteisėto tvarkymo: „Facebook“ įmonės neperžiūrėjo sąlygų ir sąlygų siūlomų programos vartotojams, siekdami įvertinti, ar tos sąlygos atitiko platformos politiką. Šią bylą išanalizavus(kurios sprendimas priimtas 2018 m. spalio 24 d.), galima būtų palyginti su jau nagrinėta duomenų politika „Facebook“, nagrinėtoje duomenų politikoje kilo neiaiškumas dėl ganėtinai abstraktaus teisėto pagrindo nustatymo (tai pat tikslų neaiškumo ir dviprasmiškumo), kuris numatė prisidėti prie pažangaus ar akademinio svarbių socialinių aspektų suvokimo, kad visuomenei ir pasauliui galėtume daryti teigiamą poveikį, o šioje byloje neteisėtas duomenų tvarkymas buvo grindžiamas moksliniais tyrimais ir produktų pagerinimu, todėl darytina išvada, kad po šios bylos sprendimo tikėtina mažai, kas pasikeitė arba aplanai niekas nepasikeitė duomenų politikoje socialiniame tinkle „Facebook“, nes kaip buvo analizuota ankstesniame skyriuje 4.1 , trūkumų ir galimų pažeidimų būtent dėl tikslo suformulavimo aptikta gana nemažai. Nurodyta, kad duomenų politika paskutinį kartą duomenų valdytojo peržiūrėta 2018 balandžio 12 d. , vadinasi galima būtų teigti, kad po šios bylos paskelbimo duomenų politika socialiniame tinkle iki šiol nėra pakeista ir pataisyta, nes bylos sprendimas priimtas 2018 m. spalio 24 d., taigi mano analizuoti 4.1 pastebėjimai ir įvardinti pažeidimai pagal BDAR galimai yra pagrįsti.

Trečioji byla susijusi su socialinio tinklo „Facebook“ „Like“ (angl. patinka) mygtuku.¹⁰² Svetainės, kurioje yra „Facebook“ mygtuko „Patinka“, operatorius gali būti duomenų valdytojas kartu su „Facebook“ rinkdamas ir perduodamas į „Facebook“ jos svetainės lankytojų asmeninius duomenis. Panašu, kad šio mygtuko įdėjimo pasekmė yra tai, kad lankytojui pasikonsultavus su „Fashion ID“ svetaine, jo lankytojo asmeniniai duomenys perduodami „Facebook Ireland“ duomenų valdytojui. Duomenų perdavimas įvyksta, kai lankytojas to nežino ir nepriklausomai nuo to, ar jis yra socialinio tinklo „Facebook“ narys, ar paspaudė mygtuką „Patinka“. Vokietijos viešųjų paslaugų asociacija „Verbraucherzentrale NRW“, kurios užduotis buvo apsaugoti ir ginti vartotojų interesus, kritikuoja „Fashion ID“ už tai, kad „Facebook Ireland“ perdavė jos tinklalapio lankytojų asmeninius duomenis, pirma, be jų sutikimo ir, antra, pažeisdama pareigą informuoti. „Fashion ID“ gali būti laikomas duomenų valdytoju kartu su „Facebook Ireland“ vykdančiomis operacijomis, susijusiomis su nagrinėjamų duomenų rinkimu ir atskleidimu perduodant juos į „Facebook Ireland“, nes tai galima padaryti (atsižvelgiant į tyrimus, kad tai yra kad „Oberlandesgericht Düsseldorf“ vykdytu). „Fashion ID“ ir „Facebook Ireland“ kartu nustato šių operacijų priemones ir tikslus. Byloje buvo pasiremta šiam darbe nagrinėta 2018 m. byla (žr. 2.2 skyrių) dėl duomenų sąvokos išplėtimo socialiniuose tinkluose. Teismas nustatė, kad „Facebook“ gerbėjų puslapio administratorius kartu su „Facebook“ yra atsakingas už duomenų, susijusių su jo puslapio lankytojais, tvarkymą. Be kita ko, atrodo, kad „Fashion ID“ įtrauktas „Facebook“ mygtukas „Patinka“ savo svetainėje leidžia optimizuoti prekių viešumą padarant jas labiau matomas „Facebook“ socialiniame tinkle, kai jos svetainės lankytojas paspaudžia tą mygtuką. Priežastis, dėl kurios, atrodo, „Fashion ID“ bent jau netiesiogiai sutiko, kad būtų renkami ir atskleidžiami jos tinklalapio lankytojų asmens duomenys, įterpiant tokį mygtuką į savo svetainę, yra ta, kad būtų galima pasinaudoti tuo komerciniu pranašumu. Taigi atrodo, kad šios duomenų tvarkymo operacijos vykdomos atsižvelgiant į „Fashion ID“ ir „Facebook Ireland“ ekonominius interesus, ir tai, kad faktas, jog ji gali naudoti šiuos duomenis savo komerciniams tikslams, yra atlygis už „Fashion ID“ naudą. Teismas aiškiai nurodo, kad tokios svetainės kaip „Fashion ID“ operatorius, kaip (jungtinis) duomenų valdytojas, atliekantis tam tikras operacijas, susijusias su jos tinklalapio lankytojų duomenų tvarkymu, pavyzdžiui, tų duomenų rinkimu ir perdavimu „Facebook“ lankytojams privalo pateikti tam tikrą informaciją, pavyzdžiui, savo tapatybę ir tvarkymo tikslus. Teismas taip pat pateikė

¹⁰² Europos Teisingumo teismas. 2019 m. liepos 12 d. byla *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Nr. C-40/17 [interaktyvus, žiūrėta 2019 m. lapkričio 3 d.]. Prieiga per internetą: < <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-07/cp190099en.pdf>>.

papildomos informacijos apie du iš šešių direktyvoje (ginčas kilo, kai galiojo 1995 m. Duomenų apsaugos direktyvos 1 nuostatų (kurios tebėra taikomos šiai bylai, tačiau dabar jas pakeitė naujasis 2016 m. bendrasis duomenų apsaugos reglamentas, įsigaliojęs nuo 2018 m. gegužės 25 d.). numatytų atvejų, kai asmens duomenų tvarkymas gali būti laikomas teisėtu. Taigi byloje, kurioje duomenų subjektas davė sutikimą, Teisingumo Teismas mano, kad tokios interneto svetainės kaip „Fashion ID“ operatorius privalo gauti šį išankstinį sutikimą (tik) operacijoms, kurioms jis yra (bendras) valdytojas, būtent duomenų rinkimas ir perdavimas. Kalbant apie atvejus, kai duomenų tvarkymas yra būtinas siekiant teisėtų interesų, Teismas konstatuoja, kad kiekvienas iš (bendrų) duomenų valdytojų, t.y., tinklalapio operatorius ir socialinio papildinio teikėjas („Fashion ID“), privalo siekti teisėto intereso įgyvendinimo renkant ir perduodant asmens duomenis, kad tos operacijos būtų pateisinamos kiekvienos iš jų atžvilgiu. Ši byla taip pat kaip ir pastaroji dėl gerbėjų puslapio nagrinėta 2018 m., dar labiau išplėčia duomenų valdytojo sąvoką ir pasako, kad duomenų valdytojai yra ne tik socialinio tinklo valdytojas, bet ir tie, kurie naudodamiesi jų mygtuku „Patinka“ komerciniais ar teisėtais duomenų tvarkymo tikslais, taip pat laikomi duomenų valdytojais.

Ketvirtoji byla yra tik prasidėjusi ir dar neišnagrinėta Austrija prieš „Facebook“. Ginčas kilęs dėl priverstinio sutikimo, konkrečiai dėl reklamos. Kaip buvo šiame darbe nagrinėta duomenų politika (žr. į 4.1 skyrių) vienas iš BDAR numatytų asmens duomenų teisės pažeidimų yra tikslo neaiškus, dviprasmiškas suformulavimas, konkrečiai tiesioginė rinkodara nėra išskiriama kaip savarankiškas duomenų tvarkymo tikslas, o implikuojama į kitus, kas nėra teisėta pagal BDAR. Todėl pateikti skundai asociacijos „NOYB“ dėl neteisėto vartotojų duomenų naudojimo reklamos tikslais arba „fiktyvaus sutikimo“¹⁰³. Pagal BDAR 7 str. Vertinant, ar sutikimas duotas laisva valia, labiausiai atsižvelgiama į tai, ar, inter alia, sutarties vykdymui, įskaitant paslaugos teikimą, yra nustatyta sąlyga, kad turi būti duotas sutikimas tvarkyti asmens duomenis, kurie nėra būtini tai sutarčiai vykdyti.

Taigi, iš naujausios ir dar negausios teismų praktikos susijusios su socialiniais tinklais nagrinėtais darbe, darytina išvada, kad asmens duomenų apsaugos teisės pažeidimų yra, tačiau taip pat BDAR normos yra išaiškinamos, kas parodo, jog pats teisės aktas nėra siauro taikymo, todėl kiekviena byla reikšminga ateityje norint labiau užtikrinti kiekvieno asmens teisę į privatumą ir į teisėtą duomenų tvarkymą pagal BDAR. Todėl kitame skyriuje bus aptarti rezultatai apklausos apie duomenų subjektus ir vertinamas jų žinojimo lygis apie asmens duomenų apsaugą naudojantis socialiniais tinklais.

¹⁰³ Asociacijos Noyb tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 6 d.]. Prieiga per internetą: < <https://noyb.eu/4complaints/>>.

4.3 Apklausoje „Asmens duomenų apsauga socialiniuose tinkluose” rezultatai

BDAR pradėtas taikyti asmens duomenų apsaugos teisėje pakankamai neseniai – nuo 2018 m. gegužės 25 d. Todėl būtų naudinga sužinoti ir įvertinti, ar socialinių tinklų vartotojai žino apie savo naujas teises ir BDAR duomenų apsaugą, ar esant pažeidimui suprastų, kad jų teisės pažeistos bei ar sugebėtų kreiptis į atitinkančią instituciją duomenų apsaugos pažeidimui išspręsti. Šios apklausoje tikslas: įvertinti, ar duomenų subjektai, aktyviai besinaudojantys socialiniais tinklais, žino apie asmens duomenų apsaugą ir, ar esant pažeidimui būtų pakankamai informuoti ir žinotų, ką daryti ir kur kreiptis. Apklausoje apklausta tikslinė auditorija, kuri naudojami socialiniais tinklais. Iš viso buvo pateikti 9 klausimai.

Šioje apklausoje (žr. į priedą nr.1) apklausta 102 žmonės, iš kurių 82,5 procentai moterų ir 17,5% vyrų, 70,6% amžiaus nuo 20-25, o 18,6% iki 30 metų. 99% apklaustųjų naudojami socialiniais tinklais kiekvieną dieną, didžioji dalis 80,8% mano, kad socialiniai tinklai turi prieigą (gali matyti, naudotis) prie privačių susirašinėjimų, nuotraukų ir pan, o 14,4% nežino, ar socialiniai tinklai turi tokią prieigą. Daugiau kaip pusė – 53% naudojami socialiniais tinklais dėl bendravimo, o kita dalis 38,3% dėl laiko praleidimo, likusieji apie 9% dėl komercinės veiklos. Didžioji dalis, kai buvo paklausti dėl socialiniuose tinkluose asmens duomenų apsaugos, atsakė, kad labai abejoja, ar tinkamai yra apsaugoti jų duomenys – 59,8%, o 34,6% atsakė, kad nežino, apsaugoti asmens duomenys. Taip pat apklaustiesiems buvo užduotas klausimas, ar žinotų, kur kreiptis esant asmens duomenų teisės apsaugos pažeidimui (konkrečiai reikėjo parašyti instituciją). Tik 7 iš 102 atsakė, jog kreiptųsi į Valstybinę duomenų apsaugos inspekciją, didžioji dalis atsakė, kad kreiptųsi į policiją, kiti į vartotojų teisių apsaugos tarnybą, o net 32 atsakė, kad tokiu atveju nežinotų, kur kreiptis. Kitu klausimu buvo norėta sužinoti, ar socialinių tinklų vartotojai žino apie BDAR ir iš kur apie jį sužinojo. 37,2% sužinojo iš žiniasklaidos, 23,1% iš darbdavio, o 28,9% nieko nežino apie tokį teisės aktą. Paskutiniu klausimu norėta išsiaiškinti, kiek vartotojų žino, kad jų asmens duomenys panaudojami tiesioginei rinkodarai – 79,4% žino, kad naudojami, o 11,8% nežino, 6,9% nežino, kad naudojami.

Taigi, galima teigti, kad didžioji dalis socialiniais tinklais naudojami kiekvieną dieną ir dėl bendravimo, todėl galima manyti, kad socialiniuose tinkluose pateikia privačią informaciją apie save, savo draugus ir artimuosius, susirašinėjimus su jais, kur dalinasi visa informacija, nuotraukomis bei taip pat pastebėtina, kad daug naudojami socialiniais tinklais dėl laiko praleidimo, kas taip pat galėtų reikšti, jog dalinamasi įvairia informacija: kur keliauja, kokiose vietose lankosi (restoranai, parduotuvės ir t.t.), p ir pan. Pastebėtina, kad

dauguma abejoja, jog jų asmens duomenys yra apsaugoti, tačiau taip pat didžioji dauguma esant pažeidimui nežino į kurią instituciją reiktų kreiptis, kas rodo, jog mažai galimai iš valstybės skirta priemonių prevenciškai šviesti visuomenę dėl asmens duomenų apsaugos ir BDAR reguliavimo. Iš šių rezultatų, galima teigti, jog apie asmens duomenų apsaugą, jos gynybos priemones ir duomenų subjektų teises nėra skirta pakankamai priemonių informuoti, todėl valstybės ir duomenų apsaugos pareigūnai privalo skirti ypatingą dėmesį užtikrinant asmens duomenų apsaugą.

IŠVADOS

1. BDAR taikymo sritis neapima absoliučiai visų duomenų apie asmenį. Kad būtų taikomos BDAR normos privalu įvertinti visumą sąlygų: bet kokia informacija apie asmenį turi būti susijusi su konkrečiu asmeniu, tas asmuo turi būti fizinis bei kurio tapatybė nustatyta arba galima būtų ją nustatyti tiesiogiai pvz.: iš vardo ir pavardės, bei netiesiogiai iš asmens kodo ar tel. numerio. BDAR taikomas socialiniams tinklams, nes vienas iš duomenų tvarkymo tikslų yra tiesioginė rinkodara, kuri reikalauja ypatingai didelio duomenų apsaugos reguliavimo dėl renkamų duomenų apie socialinių tinklų vartotojus.
2. Asmens duomenų apsauga ir privatumas nėra tapačios sąvokos ir neteisinga būtų vertinti kaip sinonimus, nes teisė į privatumą sudaro ne tik asmens duomenų apsauga, bet ir teisė į kūno neliečiamumą, teritorinę apsaugą, informacinę, kuri apima asmens duomenų apsaugą bei komunikacijų. Todėl privatumo sąvoka vertinama kaip platesnės apimties ir apimanti asmens duomenų apsaugą. Socialiniuose tinkluose nepaisant to, kad duomenų subjektai dalinasi savo jautriais duomenimis apie rasinę ar etninę kilmę, politines pažiūras, religinius ar filosofinius įsitikinimus, narystę profesinėse sąjungose arba duomenimis apie sveikatą ir lytinį gyvenimą, šių asmens duomenų viešumas nepanaikina teisės į privatumą apsaugos pagal BDAR.
3. Duomenų valdytojų sąvoka socialiniuose tinkluose ESTT išplėsta 2018 m. byloje Vokietijos regioninė duomenų apsaugos institucija prieš Vokietijos mokymo bendrovę GmbH ir apima ne tik duomenų valdytoją, kuris asmens duomenis tvarko ir nustato duomenų politiką bei technines ir organizacines priemones, bet ir tuos, kurie socialiniuose tinkluose sukuria grupes bei naudoja slapukus, suteikiančius grupių valdytojams visus duomenis apie ten prisijungusius asmenis. „Facebook“ 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 laikomas duomenų valdytoju kaip tai suprantama pagal BDAR.
4. Duomenų valdytojais laikytini naudojantys „Like“ angl. „Patinka“ mygtuką internetinėse svetainėse, nes vartotojai paspaudę šį mygtuką perduoda asmens duomenis internetiniam tinklapiui, o pastarasis socialiniam tinklui „Facebook“. ESTT nustatė, kad tokios interneto svetainės kaip „Fashion ID“ operatorius privalo gauti šį išankstinį sutikimą (tik) operacijoms, kurioms jis yra (bendras) valdytojas,

būtent duomenų rinkimas ir perdavimas. Duomenų perdavimas įvyksta, kai lankytojas to nežino ir nepriklausomai nuo to, ar jis yra socialinio tinklo „Facebook“ narys, ar paspaudė mygtuką „Patinka“. ESTT aiškiai nurodo, kad tokios svetainės kaip „Fashion ID“ operatorius, kaip (jungtinis) duomenų valdytojas, atliekantis tam tikras operacijas, susijusias su jos tinklalapio lankytojų duomenų tvarkymu, pavyzdžiui, tų duomenų rinkimu ir perdavimu „Facebook“ lankytojams privalo pateikti tam tikrą informaciją (savo tapatybę ir tvarkymo tikslus), todėl laikytinas duomenų valdytoju.

5. Socialiniame tinkle duomenų subjektų skelbiama informacija negali būti vertinama kredito mokumui nustatyti. Toks tikslas ir duomenų tvarkymas yra neteisėti pagal BDAR. LVAT pabrėžė, jog asmens duomenys gali būti tvarkomi tik esant apibrėžtiems ir teisėtiems tikslams, turi sutapti duomenų paskelbimo ir tvarkymo tikslai, turi būti užtikrintas asmens privataus gyvenimo neliečiamumas, asmens susirašinėjimas, pokalbiai telefonu, bendravimas socialiniuose tinkluose. EŽTT 2004 m. birželio 24 d. sprendime Von Hannover prieš Vokietiją pažymėjo esminę privataus gyvenimo apsaugos svarbą kiekvieno žmogaus asmenybės raidos požiūriu ir konstatavo, kad ši apsauga apima ne tik privačią šeimą, bet ir socialinę erdvę, kad kiekvienas asmuo (net jei jis ir yra žinomas plačiajai visuomenei) turi turėti galimybę naudotis teise į teisėtą lūkestį dėl savo privataus gyvenimo apsaugos ir gerbimo.
6. Atlikus duomenų politikos vertinimą „Facebook“ socialiniame tinkle pagal BDAR reikalavimus, darytina išvada, kad netinkamai, neaiškiai dviprasmiškai suformuluoti tikslai iš kurių tiesioginė rinkodara nėra išskirta kaip savarankiškas tikslas, o įvardinama kartu su kitais tikslais. Duomenų subjektų atsisakymo teisė dėl duomenų tvarkymo pateikiama neaiškiai - užsienio kalba nukreipiama nuoroda į kitą duomenų politikos puslapį. Taip pat abstrakčiai pateikiami kai kurie duomenų tvarkymo teisėtumo pagrindai neatskleidžiant esmės pvz.: socialinė gerovė ir pasauliui daromas teigiamas poveikis. Todėl „Facebook“ duomenų politiką galima vertinti kaip neatitinkančią BDAR numatytų nuostatų ir asmens duomenys gali būti tvarkomi neteisėtai.

ŠALTINIŲ SĄRAŠAS

Lietuvos Respublikos įstatymai

1. Lietuvos Respublikos Konstitucija (su pakeitimais ir papildymais). *Valstybės žinios*, 1992, Nr. 33-1014; *Lietuvos aidas*, 1992, Nr. 220 [interaktyvus, žiūrėta 2019 m. rugsėjo 30 d.]. Prieiga per internetą: <<https://www.infolex.lt/ta/72720>>.
2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios*, 1996, Nr. 63-1479 [interaktyvus, žiūrėta 2019 m. rugsėjo 21 d.]. Prieiga per internetą: <<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.29193/asr>>.
3. Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas. TAR, 2018-07-11, Nr. 2018-11745. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.299D835159BE/asr>>.
4. Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas. *Valstybės žinios*, 2002-09-18, Nr. 91-3890 [interaktyvus, žiūrėta 2019 m. rugsėjo 30 d.]. Prieiga per internetą: <<https://www.e-tar.lt/portal/lt/legalAct/TAR.817CC58C1A54>>.

ES teisės norminiai aktai

1. 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 2016 L 119, p. [interaktyvus, žiūrėta 2019 m. rugsėjo 22 d.]. Prieiga per internetą: <<https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:32016R0679&from=lt>>.
2. 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir sprendimas Nr. 1247/2002/EB. OL 2018 L p. [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <<https://eurlex.europa.eu/legalcontent/lt/txt/pdf/?uri=celex:32018r1725&from=lt>>.
3. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens

duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos paamatinis sprendimas 2008/977/TVR. OJ 2016 L 119, p. [interaktyvus, žiūrėta 2019 m. rugsėjo 26 d.]. Prieiga per internetą:<<https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:32016L0680&from=lt>>.

4. 1981 m. sausio 28 d. Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) pakeista 2018 m. gegužės 18d. protokolu (CETS Nr. 223) [interaktyvus, žiūrėta 2019 m. rugsėjo 24 d.]. Prieiga per internetą:
<<https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872>>.
5. 2012 m. Europos Parlamento, Tarybos ir Komisijos paskelbta ES pagrindinių teisių chartija [interaktyvus, žiūrėta spalio 19 d.]. Prieiga per internetą: <<https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:12012P/TXT&from=LT>>.

Specialioji literatūra:

1. ZALESKIS, Julius. *Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė*. Vilnius: VĮ registrų centras, 2019.
2. ZALESKIS, J. Duomenų apsaugos pareigūno veiklos pagrindai pagal ES Bendrąjį duomenų apsaugos reglamentą. *Teisė*, 2017.
3. CIVILKA M.; ŠLAPIMAITĖ L. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, p. 126-148.
4. MISIŪNAITĖ-KAMARAUSKIENĖ, Dalia. Europos sąjungos teisingumo teismo praktikos aktualijos pagrindinių teisių į privatų ir šeimos gyvenimą bei asmens duomenų apsaugą srityje. *Jurisprudencija*, 2014, p. 1233–1245.
5. MALINAUSKAITĖ-VAN DE CASTEL, Inga. *Duomenų subjekto teisės virtualiuose socialiniuose tinkluose: daktaro disertacija*. Socialiniai mokslai, teisė (01 S). Vilnius: Mykolo Romerio universitetas, 2017.
6. SIRBIKYTĖ, Gintarė. Ar socialinio tinklo valdytojas atsako už šio tinklo naudotojo neteisėtais veiksmais padarytą žalą? *Teisės apžvalga*, 2013, p. 30-85.
7. SABAITYTĖ, J.; KARPORAVIČIŪTĖ, R. Didžiųjų duomenų panaudojimas socialinėje medijoje. *Mokslas – Lietuvos ateitis*, 2019, p.1–13.
8. PETRAITYTĖ, Ilona. *Asmens duomenų teisinės apsaugos principai: daktaro disertacija*. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.

9. PETRAITYTĖ, Ilona. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*. 2011, p. 166.
10. SAVICKA, Aida. Virtualūs socialiniai tinklai: viešumo ir privatumo problematika. *Lietuvos kultūros tyrimai*. 2012, p. 157.
11. JURKEVIČIENĖ, Jurgita. *Elektroniniai socialiniai tinklai naujosiose socialinėse medijose: dalyviai ir jų veiklos*: daktaro disertacija. Socialiniai mokslai, sociologija (05S) p.17-18.
12. KIŠKIS, Mindaugas. Socialiniai iššūkiai tiesioginei elektroninei rinkodarai. *Ekonomika ir vadyba*. 2009, p. 430–440.
13. JEZUKEVIČIŪTĖ, J.; DAVIDAVIČIENĖ, V. Prekės ženklo rinkodaros modelis socialiniuose tinkluose. *Mokslas – lietuvos ateitis*, 2014, p.122.
14. HIATT D., B.CHOI Y. Role of Security in Social Networking (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, 2016, p.13.

Teismų praktika

1. Lietuvos Vyriausiojo administracinio teismo teisėjų kolegija. 2016 m. birželio 13 d. nutartis administracinėje byloje UAB „Creditinfo Lietuva“ v. Valstybinė duomenų inspekcija, Nr. A-408-858/2016.
2. ES Teisingumo teismas. 2018 m. birželio 5 d. sprendimas *Vokietijos regioninė duomenų apsaugos institucija v. Vokietijos mokymo bendrovę GmbH* [interaktyvus, žiūrėta 2019 m. rugsėjo 16 d.]. Prieiga per internetą: <<http://curia.europa.eu/juris/document/document.jsf?text=&docid=202543&pageIndex=0&doclang=LT>>.
3. ES Teisingumo teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain ir Google*, 34 p. [interaktyvus, žiūrėta 2019 m. spalio 1 d.]. Prieiga per internetą:<<http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=LT>>.
4. Lietuvos Respublikos Konstitucinis teismas. 2000 m. gegužės 8 d. nutarimas *Dėl Lietuvos Respublikos operatyvinės veiklos įstatymo 2 straipsnio 12 dalies, 7 straipsnio 2 dalies 3 punkto, 11 straipsnio 1 dalies ir Lietuvos Respublikos baudžiamojo proceso kodekso 198¹ straipsnio 1 bei 2 dalių atitikimo Lietuvos Respublikos Konstitucijai*, Nr. 12/99-27/99-29/99-1/2000-2/2000.
5. Europos Teisingumo teismas. 2019 m. liepos 12 d. sprendimas *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV*, Nr. C-40/17 [interaktyvus, žiūrėta 2019 m. lapkričio 3 d.]. Prieiga per internetą:

<https://curia.europa.eu/jcms/upload/docs/application/pdf/201907/cp190099en.pdf>

6. Lietuvos Respublikos Konstitucinis teismas. 2011 m. Birželio 9 d. Nutarimas dėl Lietuvos Respublikos nekilnojamojo turto registro įstatymo (2001 m. Birželio 21 d. Redakcija) 42 straipsnio atitikties Lietuvos Respublikos Konstitucijai ir Lietuvos Respublikos vyriausybės 2002 m. Liepos 12 d. Nutarimu nr. 1129 „Dėl nekilnojamojo turto registro nuostatų patvirtinimo“ patvirtintų nekilnojamojo turto registro nuostatų 88 punkto (2007 m. Vasario 27 d. Redakcija), 97 punkto (2007 m. Vasario 27 d., 2008 m. Spalio 22 d., 2010 m. Kovo 3 d., 2011 m. Gegužės 4 d. Redakcijos) atitikties Lietuvos Respublikos Konstitucijai, Nr. 12/2008-45/2009.
7. Lietuvos Aukščiausiojo teismo Civilnių bylų skyriaus kolegija. 2013 m. birželio 19 d. D.J v. V.J ir J.B, Nr. 3K-3-336/2013.
8. Lietuvos vyriausiojo administracinio teismo teisėjų kolegija. 2017 m. lapkričio 21 d. S.F v. Vilniaus miesto savivaldybės administracija, Nr. AS-1003-756/2017.
9. Lietuvos Respublikos Konstitucinis teismas. 2008 m. sausio 22 d. nutarimas dėl Lietuvos Respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl priėmimo į valstybės tarnautojo pareigas tvarkos patvirtinimo“ (2002 m. Birželio 24 d., 2002 m. Rugsėjo 29 d., 2003 m. Birželio 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. Balandžio 23 d. Redakcija) 1 daliai, dėl Lietuvos Respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2006 m. Birželio 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. Balandžio 23 d., 2007 m. Birželio 7 d. Redakcijos) 1 daliai, taip pat dėl Lietuvos Respublikos vyriausybės 2002 m. Birželio 24 d. Nutarimu nr. 966 „dėl konkursų į valstybės tarnautojo pareigas organizavimo tvarkos aprašo patvirtinimo“ (2007 m. Rugsėjo 26 d., 2007 m. Gruodžio 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. Birželio 7 d. Redakcija) 1 daliai.
10. Lietuvos Respublikos Konstitucinio Teismo. 2010 m. birželio 29 d. nutarimas dėl Lietuvos Respublikos teisėjų valstybinių pensijų įstatymo 5, 6 straipsnių, Lietuvos

Respublikos valstybinių pensijų įstatymo 3 straipsnio 3 dalies (2009 m. gruodžio 8 d. redakcija), Lietuvos Respublikos socialinių išmokų perskaičiavimo ir mokėjimo laikinojo įstatymo 1 straipsnio 2 dalies 1 punkto, 16 straipsnio 4 dalies atitikties Lietuvos Respublikos Konstitucijai, Nr. 134-6860.

11. Lietuvos Respublikos Konstitucinis teismas. 2011 m. sausio 31 d. nutarimas dėl Lietuvos Respublikos civilinio kodekso 4.103 straipsnio (2006 m. spalio 17 d. redakcija) 3 dalies ir Lietuvos Respublikos statybos įstatymo 28 straipsnio (2006 m. spalio 17 d., 2009 m. lapkričio 19 d. redakcijos) 3 dalies atitikties Lietuvos Respublikos Konstitucijai, Nr. 14-602.
12. 2018 m. spalio 24 d. Facebook Ireland Ltd penalty notice [interaktyvus, žiūrėta 2019 m. lapkričio 6 d.]. Prieiga per internetą: < <https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf>>.

ES soft law šaltiniai

1. 2017 m. lapkričio 28 d. ES 29 str. darbo grupės gairės dėl sutikimo pagal Reglamentą (ES) 2016/679 Nr. WP259 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <
2. 2016 m. liepos 19 d. ES 29 str. darbo grupės nuomonė Nr. 03/2016 dėl ES e. privatumo direktyvos 2002/58/EB Nr. WP240 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą:<https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf>.
3. 2016 m. gruodžio 13 d. ES 29 str. darbo grupės gairės dėl duomenų perkeliavimo nr. WP242, p.4 [interaktyvus, žiūrėta 2019 m. lapkričio 19 d.]. Prieiga per internetą: <https://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp242_en_40852.pdf>.
4. 2017 m. ES 29 str. darbo grupės gairės dėl skaidrumo [interaktyvus, žiūrėta 2019 m. spalio 18 d.]. Prieiga per internetą: <https://iapp.org/media/pdf/resource_center/wp29-transparency-12-12-17.pdf>.
5. 2014 m. balandžio 9 d. ES 29 str. darbo grupės nuomonė Nr. 06/2014 dėl duomenų valdytojo teisėtų interesų sampratos pagal Direktyvos 95/46/EB 7 str. Nr. WP217 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>.
6. 2013 m. balandžio 2 d. ES 29 str. darbo grupės nuomonė Nr. 03/2013 dėl tikslo apribojimo Nr. WP203 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per

- interneta: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf>.
7. 2011 m. liepos 13 d. ES 29 str. darbo grupės nuomonė dėl sutikimo apibrėžimo Nr. WP187 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf>.
 8. 2010 m. gruodžio 16 d. ES 29 str. darbo grupės nuomonė Nr. 8/2010 dėl taikytinos teisės Nr. WP179 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf>.
 9. 2010 liepos 13 d. ES 29 str. darbo grupės nuomonė Nr. 3/2010 dėl atskaitomybės principo, p.4 [interaktyvus. Žiūrėta 2019 m. lapkričio 1 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf>.
 10. 2010 m. vasario 16 d. ES 29 str. darbo grupės nuomonė Nr. 1/2010 dėl sąvokų „duomenų valdytojas“ ir „duomenų tvarkytojas“ Nr. WP169 [interaktyvus. žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_lt.pdf>.
 11. 2009 m. birželio 12 d. ES 29 str. darbo grupės nuomonė Nr. 5/2009 dėl socialinių tinklų WP163 [interaktyvus, žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2009/wp163_en.pdf>.
 12. 2007 m. birželio 20 d. ES 29 str. darbo grupės Nuomonė Nr. 4/2007 dėl asmens duomenų sąvokos Nr. WP136 [interaktyvus. žiūrėta 2019 m. rugsėjo 20 d.]. Prieiga per internetą: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
 13. 2016 m. liepos 12 d. Europos Komisijos įgyvendinimo sprendimas (ES) 2016/1250 ir dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo pagal Europos Parlamento ir Tarybos direktyvą 95/46 (pranešta dokumentu Nr. C(2016) 4176). OL 2016 L 207, p. [interaktyvus, žiūrėta 2019 m. rugsėjo 19 d.]. Prieiga per internetą: <<https://eurlex.europa.eu/legalcontent/LT/TXT/PDF/?uri=CELEX:32016D1250&from=LT>>.
 14. 1970 m. sausio 23 d. Europos Tarybos Parlamentinės Asamblėjos rezoliucija Nr. 428/1970 „Dėl masinės informacijos priemonių ir žmogaus teisių“. [interaktyvus, žiūrėta 2019 spalio 3d.]. Prieiga per internetą: <

<http://assembly.coe.int/nw/xml/XRef/XrefXML2HTMLen.asp?fileid=15842&lang=en>.

15. 2014 m. birželio 14 d. ES 29 str. darbo grupės nuomonė Nr.0829/14 dėl nuasmeninimo metodų [interaktyvus, žiūrėta 2019 m. spalio 30 d.]. Prieiga per internetą: <<https://www.pdpjournals.com/docs/88197.pdf>>.

Kiti šaltiniai

1. The history of social networking: how it all began [interaktyvus, žiūrėta 2019 m. rugpjūčio 18 d.]. Prieiga per internetą: <<https://1stwebdesigner.com/history-of-social-networking/>>.
2. HSIEH, C.; CHEN, S. *A Cognitive Style Perspective to Handheld Devices: Customization vs. Personalization* [interaktyvus, žiūrėta 2019 m. rugsėjo 2 d.]. Prieiga per internetą: <<https://files.eric.ed.gov/fulltext/EJ1090869.pdf>>.
3. TeisėPro internetinis tinklapis. [interaktyvus, žiūrėta 2019 m. spalio 2 d.]. Prieiga per internetą: <<http://www.teise.pro/index.php/2018/06/05/m-rudyte-bdar-kodel-svarbu-atskirti-duomenu-valdytoja-nuo-tvarkytojo/>>.
4. Oficiali Europos Sąjungos svetainė [interaktyvus, žiūrėta 2019 m. spalio 26 d.]. Prieiga per internetą: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/how-much-data-can-be-collected_lt>.
5. Guide to the general data protection [interaktyvus, žiūrėta 2019 m. spalio 30 d.]. Prieiga per internetą: <<https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf>>.
6. Duomenų politika [interaktyvus, žiūrėta 2019 m. spalio 29 d.]. Prieiga per internetą: <<https://lt-lt.facebook.com/help/instagram/155833707900388>>.
7. Statista tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 8 d.]. Prieiga per internetą: <<https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/>>.
8. GDPR tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 7 d.]. Prieiga per internetą: <<https://gdpr.lt/>>.
9. Danah Boyd ir Nicole Ellison publication history [interaktyvus, žiūrėta 2019 m. lapkričio 8 d.]. Prieiga per internetą: <<https://onlinelibrary.wiley.com/doi/full/10.1111/j.1083-6101.2007.00393.x>>.
10. Asociacijos Noyb tinklapis [interaktyvus, žiūrėta 2019 m. lapkričio 6 d.]. Prieiga per internetą: <<https://noyb.eu/4complaints/>>.

11. C/net tinklapis [interaktyvus, žiūrėta 2019 lapkričio 18 d.]. Prieiga per internetą:
<<https://www.cnet.com/news/facebook-to-build-custom-audiences-tool-to-fight-advertising-without-consent/>>.

SANTRAUKA (lietuvių kalba)

Šiame darbe analizuojamos BDAR nuostatos dėl duomenų valdytojo pareigų ir duomenų subjektų teisių įgyvendinimo ir taikymo socialiniame tinkle „Facebook“. Didžiausias dėmesys skiriamas ES 29 str. darbo grupės nuomonių išaiškinimams apie BDAR teisės normų taikymą. Analizuojama asmens teisė į privatumą ir santykis su asmens duomenų apsauga, atskleidžiamas duomenų valdytojo ir duomenų tvarkytojo BDAR normų turinys ir takoskyra tarp šių sąvokų. Darbe atskleidžiami pagrindiniai duomenų apsaugos teisės principai: teisėtumo, sąžiningumo ir skaidrumo principas asmens duomenų apsaugoje duomenų tvarkymo tikslo apribojimo principo įgyvendinimas socialiniuose tinkluose duomenų kiekio mažinimo pareiga, duomenų tikslumo principo privalomumas, saugumo užtikrinimas ir atskaitomybės pareiga. Taip pat analizuojama naujausia teismų praktika susijusi su „Facebook“ socialiniu tinklu ir pateikiami ypatumai susiję su BDAR normų taikymu. Remiantis teoriniu metodu nagrinėjama dabartinė socialinė tinklo „Facebook“ duomenų politika ir pateikiamos bendros išvados išanalizavus norminę, specialiąją literatūrą, teismų praktiką ir teisės doktriną apie BDAR taikymą socialiniame tinkle „Facebook“.

SUMMARY (anglų kalba)

The Master's thesis analyzes GDPR's provisions on the implementation and enforcement of data controller responsibilities and data subjects' rights on Facebook. The main attention is given to a huge amount of articles 29 working group data protection working party. In the thesis is analyzed the individual's right to privacy and the coherence to the protection of personal data and the content of the GDPR'S norms. This thesis reveals the basic principles of data protection law: the principles of lawfulness, fairness and transparency in personal data protection implementation of the purpose limitation principle on data processing in social networks and accountability. It also analyzes recent cases related to Facebook's social network and presents features related to the application of GDPR norms. Based on the theoretical approach, the current social data policy of Facebook is analyzed and general conclusions are drawn from the analysis of normative, specialized literature, case law, and legal doctrine on the application of GDPR's on Facebook.

PRIEDAS NR. 1 APKLAUSOS “ASMENS DUOMENŲ APSAUGA SOCIALINIUIOSE TINKLUOSE” REZULTATAI

Asmens duomenų apsauga socialiniuose tinkluose

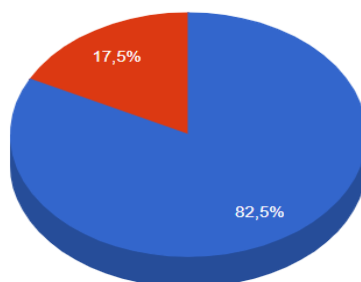
« Mano anketų sąrašas Anketos nustatymai Klausimai Rezultatai (102) HTML

Trūksta atsakymų? Reikia didesnio respondentų aktyvumo?

Grafikas

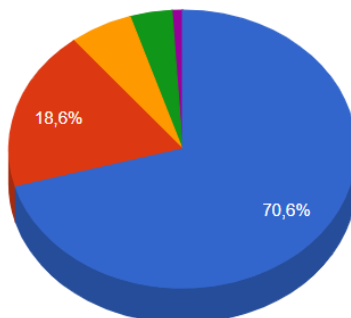
Kokia yra Jūsų lytis?

- Moteris
- Vyras



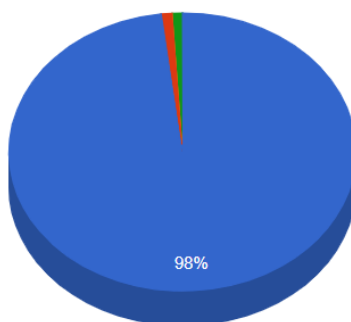
Koks Jūsų amžius?

- Nuo 20-25
- Nuo 26-30
- Nuo 31-40
- Nuo 41-50
- Neatsakė į klausimą



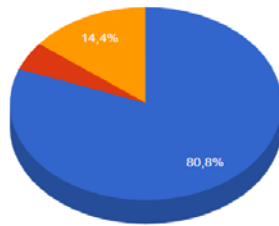
Ar naudojātės socialiniais tinklais?

- Taip, kiekvieną dieną
- Taip, kas kelias dienas
- Taip, kas savaitę
- Taip, kas mėnesį ar rečiau
- Nesinaudoju



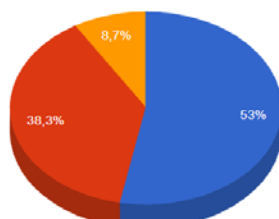
Kaip manote, ar socialiniai tinklai turi prieigą (gali matyti, naudotis) prie jūsų privačių susirašinėjimų, nuotraukų ir pan.?

- Taip, turi
- Ne, nes apsaugoti tokie duomenys
- Nežinau



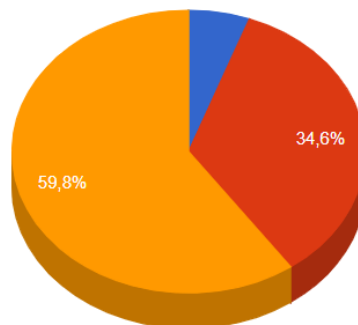
Kodėl naudojate socialiniais tinklais?

- Del bendravimo
- Del laiko praleidimo
- Del komercinės veiklos



Kaip manote, ar Jūsų asmens duomenys socialiniuose tinkluose yra tinkamai apsaugoti??

- Taip
- Ne
- Labai abejoju

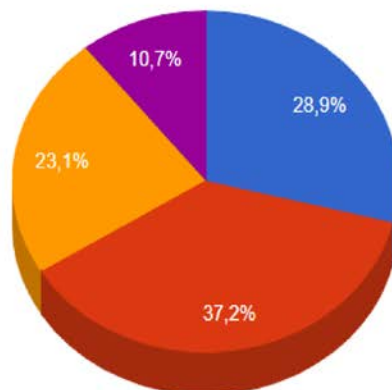


Ar žinote, kur kreiptumėtės, jei Jūsų asmens duomenų saugumas būtų pažeistas? Jei taip, nurodykite institucijas, kur kreiptumėtės.

- Ne
- Ne. Pasigooglinčiau
- I policija
- ne
- VDAI
- Nežinau
- į valstybinę duomenų apsaugos inspekciją?
- Tiesiogiai i socialine platforma.

Iš kur sužinojote apie Bendrąjį duomenų apsaugos reglamentą?

- Nieko nežinau
- Iš žiniasklaidos
- Iš darbdavio
- Iš kaimyno
- Iš draugo/draugės



Kaip manote, ar Jūsų duomenys (pvz.: pamėgti arba naršomi puslapiai, grupėse, kuriose esate, ką komentuojate ir pan.) socialiniuose tinkluose yra panaudojami tiesioginiai rinkodarai ir reklamai?

- Taip, naudojami
- Ne, nenaudojami
- Nežinau
- Neatsakė į klausimą

