MYKOLO ROMERIO UNIVERSITETO
VIEŠOJO SAUGUMO AKADEMIJA

LINAS JUDŽENTAS
TEISĖ IR POLICIJOS VEIKLA

SOCIALINIAI TINKLAI IR ASMENS PRIVATUMO SAUGA

Magistro baigiamasis darbas

Vadovas: prof. dr. Birutė Pranevičienė

.....

Darbo autorius: L. Judžentas

.....

Kaunas, 2021

TURINYS

ĮVADAS

Temos naujumas ir aktualumas. Informacinė visuomenė sukūrė įvairias nuotolinės prieigos prie paskirstytų informacijos išteklių ir vartotojų komunikacijos galimybes (virtuali aplinka, debesijos paslaugos, socialinė žiniasklaida ir kt.). Visi šie globalizacijos produktai skatina asmenis kurti savo virtualų profilį, pateikiant savo asmens duomenis ir/ar dalinantis asmenine informacija[1]. Kyla klausimas, ar šie duomenys tinkamai apsaugoti? Tai – svarbus klausimas, kurį kiekvienas asmuo turėtų sau užduoti.

Socialiniuose tinkluose susiformavo ir besivysto ypatinga bendravimo terpė. Prieiga prie asmeninių nuomonių, asmeninės informacijos dabar yra galima su ir be socialinių tinklų vartotojų žinios[2], todėl asmens privatumo saugos užtikrinimas yra didelis iššūkis ne tik socialinių tinklų vartotojams, bet ir jas valdančioms organizacijoms[3]. Pažeidimai socialiniuose tinkluose asmens privatumo saugumo srityje gali būti susiję su tikslingai netinkamu vartotojų duomenų naudojimu siekiant pelno, arba dėl saugumo trūkumų, kas tyčia ar netyčia leido trečiosioms šalims naudotis šiais duomenimis[4]. „Facebook“ ne kartą buvo kaltinamas, kad be privataus asmens sutikimo perleido informaciją apie jį tretiesiems asmenims[5]. Asmens teisės į privatumą pažeidimų atvejai socialiniuose tinkluose, įskaitant ir skandalingai nuskambėjusį „Cambridge Analytica“ atvejį, rodo, kad egzistuoja reali teisės į privatų gyvenimą pažeidimo grėsmė, todėl tinklų valdytojams privalu imtis apsaugos priemonių.

Socialinių tinklų valdymo organizacijos palaipsniui didino privatumo užtikrinimo mechanizmų pasiūlą, siekiant apsaugoti asmenų privatumą ir vykdyti įsipareigojimus. Socialinius tinklus valdančios organizacijos teikia oficialius pranešimus, kuriuose pristatomi esami ir atnaujinti įsipareigojimai dėl asmens privatumo saugos, taip pat apie saugos gerinimo politiką[6]. Saugai užtikrinti taikomos trečiųjų šalių privatumo apsaugos sertifikavimo sistemos, tokios kaip TRUSTe, BBBOnline ir WebTrust, kurios veikia kaip automatiniai saugikliai, siekianti atitikti teisės aktų nustatytiems apsaugos standartams[7]. Taip

---

[1] Radi Romansky, „Social media and personal data protection“, *International Journal on Information Technologies & Security*, 4 (2014): 65–80.

[2] Jiang Zhenhui, Cheng Suang Heng, Ben CF Choi, „Research note – privacy concerns and privacy – protective behavior in synchronous online social interactions“, *Information Systems Research* 24, (2013): 579–595.

[3] Danah M. Boyd, Nicole B. Ellison, „Social network sites: definition, history, and scholarship“, *IEEE English Management Review* 38 (3) (2010): 16–31.

[4] Alyssa Newcomb, „A timeline of Facebook's privacy issues and its responses“, NBC News, žiūrėta 2020 m. rugsėjo 1 d., https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.

[5] Josh Edelson, „A timeline of Facebook's privacy issues and its responses“, NBC News, žiūrėta 2020 m. rugsėjo 1 d., https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-re-sponses-n859651.

[6] Reza Mousavi, Rui Chen, Dan J. Kim, Kuanchin Chen, „Effectiveness of privacy assurance mechanisms in users' privacy protectionon social networking sites from the perspective of protection motivation theory“, *Decision Support Systems* 135 (2020): 1–14.

[7] Elias Baltassis, John Rose, Antoine Gourevitch, „Leveraging GDPR to become a trusted data steward, The Boston Consulting Group, žiūrėta 2020 m. rugsėjo 1 d., https://www.bcg.com/en-us/publications/2018/leveraging-gdpr-be-come-trusted-data-steward.aspx.

pat svetainėse taikomos pasirenkamos privatumo sąlygos: patys asmenys gali pakeisti būdą, kaip renkami, saugomi ir viešinami jų duomenys, arba kaip ištrinti savo paskyras. Kiekvienas iš šių privatumo užtikrinimo mechanizmų skirtingai kontroliuoja ir saugo asmenų privatumą.

Rašant darbą remtasi Lietuvos ir užsienio mokslininkų darbais. Apie teisę į privatų gyvenimą rašoma Ilonos Petraitytės[8], Ingos Malinauskaitės[9], Liudvikos Meškauskaitės ir Mindaugo Lankausko[10] darbuose. Apie asmens privatumo saugą socialiniuose tinkluose, šios teisės įgyvendinimo problemas rašoma Danah M. Boyd ir Nicole B. Ellison[11], Michael Beye ir kt.[12], Jiang Zhenhui ir kt.[13], Radi Romansky[14], Ingos Malinauskaitės[15], Mindaugo Civilkos ir Linos Šlapimaitės[16], Reza Mousavi ir kt.[17] darbuose. Taip pat darbui aktualūs tarptautiniai, Europos Sąjungos bei Lietuvos teisės aktai, reglamentuojantys socialinių tinklų veiklą saugant asmenų teisę į privatumą. Pateikiamas bei vertinamas ne tik minėtų teisės aktų, bet ir teismų praktikos, formuojančios socialinių tinklų valdytojų atsakomybės už asmenų teisės į privatų gyvenimą klausimus, reglamentavimas.

Pažymėtina, jog teisinėje mokslinėje literatūroje pasigendama naujos, išsamesnės ir gilesnės analizės, siekiant nagrinėti asmens privatumo saugos socialiniuose tinkluose teisinį reguliavimą, susistemintų teismų praktiką nagrinėjama tema, identifikuotų probleminius aspektus. Lietuvos mokslininkų indėlis nagrinėjama tema yra nepakankamas. Teisinėje literatūroje pasigendama tyrimų, diskusijų šia tema. Taip pat trūksta diskusijų, platesnio analizės lauko. Tyrimu atskleidžiama apie naują, aktualią ir nepakankamai tyrinėtą asmens privatumo reiškinio dalį – asmens privatumo saugą socialiniuose tinkluose.

Darbas gali būti naudingas mokslininkams, kurie nagrinėja asmens privatumo saugos socialiniuose tinkluose teisinį reguliavimą, taip pat studentams, kurie siekia gilinti žinias šioje srityje.

---

[8] Ilona Petraitytė, „Asmens duomenų apsauga ir teisė į privatų gyvenimą“, *Teisė* 80 (2011): 163 – 174.

[9] Inga Malinauskaitė, „Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė“, *Social Transformations in Contemporary Society* 3, (2015): 115 – 127.

[10] Liudvika Meškauskaitė, Mindaugas Lankauskas, „Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos žmogaus teisių teismo bei Lietuvos teismų praktikos kontekste“, *Teisės problemo*s 1, 91 (2016): 52 – 80.

[11] Danah M. Boyd, Nicole B. Ellison, „Social network sites: definition, history, and scholarship“, *IEEE English Management Review* 38 (3) (2010): 16–31.

[12] Michael Beye et al., „*Literature Overview - Privacy in Online Social Networks*“, Computational Social Networks (Springer: 2012): 87–113.

[13] Jiang Zhenhui, Cheng Suang Heng, Ben CF Choi, „Research note – privacy concerns and privacy – protective behavior in synchronous online social interactions“, *Information Systems Research* 24, (2013): 579–595.

[14] Radi Romansky, „Social media and personal data protection“, *International Journal on Information Technologies & Security*, 4 (2014): 65–80.

[15] Inga Malinauskaitė, „Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė“, *Social Transformations in Contemporary Society* 3, (2015): 115 – 127.

[16] Mindaugas Civilka, Lina Šlapimaitė, „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė* 96, (2015): 126 – 148.

[17] Reza Mousavi, Rui Chen, Dan J. Kim, Kuanchin Chen, „Effectiveness of privacy assurance mechanisms in users' privacy protectionon social networking sites from the perspective of protection motivation theory“, *Decision Support Systems* 135 (2020): 1–14.

Tyrimo problema. Dėl socialinių tinklų plėtros ir informacinių technologijų priemonių taikymo juose pažangos, privačiam asmeniui itin sudėtinga užtikrinti saugią aplinką, kurioje būtų tinkamai ginama jo teisė į privatumą.

Tyrimo tikslas – išanalizuoti asmens privatumo saugos socialiniuose tinkluose teisinio reguliavimo problematiką.

Tyrimo objektas – asmens privatumo sauga socialiniuose tinkluose.

Tyrimo dalykas – asmens privatumo saugos socialiniuose tinkluose teisinio reguliavimo probleminiai aspektai.

Tyrimo uždaviniai:

1. Pateikti teisės į privatų gyvenimą koncepcijos probleminius aspektus.
2. Pristatyti asmens privatumo saugos teisinio reguliavimo raidą.
3. Analizuoti asmens privatumo saugos socialiniuose tinkluose ypatumus.
4. Išanalizuoti asmens privatumo saugos socialiniuose tinkluose įgyvendinimo problemas praktikoje.

Tyrimo klausimas. Ar esamas tarptautinis ir nacionalinis teisinis asmens privatumo saugos teisinis reguliavimas yra pakankamas siekiant užtikrinti asmens privatumą socialiniuose tinkluose?

Darbe taikomi tyrimo metodai:

- abstrakcijos, dedukcijos ir sintezės metodai taikomi, siekiant paaiškinti darbe naudojamas sąvokas, mokslinėje literatūroje, teisės aktuose, įtvirtintų nuostatų pobūdį, susijusių su analizuojama tema;
- apibendrinimo metodas naudojamas sisteminant informaciją, gautą analizuojant aktualius teisės šaltinius, teismų praktiką;
- dokumentų analizės metodas pasitelkiamas, nes renkami duomenys tema „Socialiniai tinklai ir asmens privatumo sauga“, o dokumentai naudojami kaip pagrindiniai informacijos šaltiniai, pasirinktos temos problematikai atskleisti;
- lyginimo metodas taikytas išryškinant tarptautinių ir nacionalinių teismų teisminę praktiką ir teisės doktriną.

Darbo struktūra. Magistro baigiamąjį darbą sudaro keturios dalys. Pirmoje magistro darbo dalyje pateikiami teisės į privatų gyvenimą koncepcijos probleminiai aspektai, analizuojant teisės į privatų gyvenimą sampratą, turinį, privatumo ribas, asmens privatumo užtikrinimo principus ir priemones. Antroje magistro baigiamojo darbo dalyje pristatoma asmens privatumo saugos tarptautinio ir nacionalinio teisinio reguliavimo raida ir probleminiai aspektai. Trečioje darbo dalyje analizuojami

asmens privatumo saugos socialiniuose tinkluose pažeidimo ir užtikrinimo būdai. Ketvirtoje darbo dalyje analizuojama teismų praktika, kurioje ginamas asmens privatumas socialiniuose tinkluose. Darbo pabaigoje pateikiamos magistro baigiamojo darbo išvados, siūlymai, anotacija bei santrauka lietuvių ir anglų kalbomis.

1. ASMENS PRIVATUMO SAUGOS KONCEPCIJA

1.1. Teisės į privatų gyvenimą samprata ir turinys

Europos žmogaus teisių teismas (toliau – EŽTT) ilgai vengė formuluoti privataus gyvenimo apibrėžimą, teigdamas, kad nėra nei galimybės, nei būtinybės išsamiai apibrėžti privataus gyvenimo sąvoką. Kaip teigia Toma Razmaitė[18], kiekvienas individualiai ir subjektyviai vertina, kas jų gyvenime yra privatu, vieša, o teismas, priimdamas sprendimą, kiekvienu atskiru atveju sprendžia, kas yra privatus gyvenimas ir, kada jis yra pažeistas. Privatumui būdingas subjektyvumas, kas apsunkina privatumo sąvokos apibrėžimą.

EŽTT teisės į privatų gyvenimą sąvoką aiškina per privačiam gyvenimui būdingus požymius.

EŽTT byloje Pretty prieš Jungtinę Karalystę[19] pateikė privataus gyvenimo apibrėžimą, teigdami, kad „terminas „privatus gyvenimas" yra plati sąvoka, neturinti išsamaus apibrėžimo. Ši sąvoka asmens fizinės ir psichinės būklės aspektus. Taip pat privatus gyvenimas glaudžiai susijęs su psichologiniais aspektais, socialiniu statusu, kaip kalbama apie asmens lytį, šeiminę padėtį, seksualinę orientaciją ir kt. Šiuos, su asmeniu susijusiu aspektus, gina EŽTK 8 str. Taip šis straipsnis užtikrina teisę siekti asmeninio tobulėjimo, būti kūrybiškam, užmegzti santykiais su kitais. EŽTT byloje Niemietz prieš Vokietiją[20] pateikė dar keletą privataus gyvenimo turinį nusakančių požymių. EŽTT išreiškė nuomonę, kad privatus gyvenimas tai ne tik žmogaus „intymus ratas", kuriame kiekvienas turi teisę ir gali elgtis kaip jam atrodo tinkama, atsiribojant nuo jį supančio pasaulio, tai taip pat šio asmens gyvenimo gerbimas, jo teisė kurti santykius su žmonėmis profesinėje ir kasdienėje veikloje. EŽTT pabrėžė, kad būtent darbo vietoje asmuo gali užmegzti daug išorinių socialinių ryšiu. Kaip pažymi Mindaugas Civilka ir Rita Barasnevičiūtė[21], teisė į privatų gyvenimą vis labiau grindžiama socialiniais santykiais, bendravimu, ryšių tarp asmenų palaikymu, plėtojimu, bendradarbiavimu, o ne atsiskyrimu ir atitolimu vienam nuo kito.

Asmuo turi teisę į privatų gyvenimo, kaip ir į teisę, kaip informacija apie asmenį būtų apsaugota. Europos Tarybos Generalinė Asamblėja rezoliucijoje 428/1970 „Dėl masinės informacijos priemonių"[22] teisės į privatų gyvenimą turinį papildė tokiais požymiais kaip: asmens garbė, reputacija, asmeninių faktų slaptumas, draudimas be leidimo publikuoti asmens atvaizdą (nuotrauką), draudimas skelbti gautą ar

[18] Toma Razmaitė, „*Google street view" atvejis: teisės į privatumą ir technologijų plėtros santykis*" (Vilnius: MRU, 2014): 15.
[19] Pretty prieš Jungtinę Karalystę, Application No. 2346/02. 2002.
[20] Niemietz prieš Vokietiją, Application No. 13710/88. 1992.
[21] Mindaugas Civilka, Rita, Baresnevičiūtė, „Asmens duomenų apsauga ir privatumas: sąveika su informacinės visuomenės aktualijomis", *Justitia, 4* (2007): 66.
[22] „Europos Tarybos Generalinė Asamblėjos rezoliucija Nr. 428/1970 „Dėl masinės informacijos priemonių", žiūrėta 2020 m. lapkričio 1 d., http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en.

surinktą konfidencialią informaciją. Kaip teigiama Peck prieš Jungtinė Karalystę byloje[23], EŽTK 8 str. gina asmens teises į privatumą, publikuojant viešosiose vietose surinktas nuotraukas, vaizdo įrašus, kuriuose yra asmens atvaizdas.

Lietuvos Respublikos Konstitucinis Teismas (toliau – LR Konstitucinis Teismas) nesiryžo suformuluoti privataus gyvenimo apibrėžimą, teigdamas, kad „žmogaus privatus gyvenimas – sritis, kuri būtent dėl savo grynai asmeninio, emocinio pobūdžio negali būti formalizuota, apibrėžta privalomomis vykdyti taisyklėmis“[24]. LR Konstitucinis Teismas 1999 m. spalio 21 d. nutarime[25] pasisakė, kad EŽTT pakankamai aiškiai ir plačiai apibrėžė privatumo apimtis ir turinį. LR Konstitucinio Teismo nutarime[26] teigiama, kad žmogaus privatų gyvenimą apima informaciją apie jo šeiminę padėtį, pažiūras, elgseną ir jos pokyčius, įpročius, gyvenimo būdą, aplinką, kurioje gyvenama, socialinius ryšius, sveikatos būklę, orumą ir kt. Teisė į privatų gyvenimą apima neliečiamybės užtikrinimą toms sritims, kurias apima žmogaus privatus gyvenimo turinys: asmeniniai duomenys, gyvenimas šeimoje, reputacija, fizinė ir psichinė būklė, ir kt., bei apsaugą joms, siekiant drausti kitiems gauti ir skelbti informaciją apie asmenį. Anot Liudvikos Meškauskaitės ir Mindaugo Lankausko[27], LR Konstitucinis Teismas plačiau apibūdina privataus gyvenimo bei teisės į privatumą turinį, pateikdamas didesnį kiekį asmens privatumo sričių, nors šios sritys nėra apibūdinamos griežtai ir tiksliai. LR Konstitucinio Teismo ir EŽTT požiūris į privatų gyvenimą ir jo turinį yra panašus, tačiau abi institucijos atsargiai formuluoja privataus gyvenimo ir teisės į privatų gyvenimą sąvokų apibrėžtis, kadangi aiškinant jas galima labai plačiai interpretuoti, kas yra asmeniui yra privatu, ir kas ne, kur teisė yra ginama, o kur yra viešas interesas.

Apibendrinant galima teigti, kad asmens privatus gyvenimas ne tik jo asmeninė, nuošali erdvė, į kurią neturi teisės ir nesikiša tretieji asmenys, tačiau tai ir žmogaus santykiai su socialine aplinka, informacija apie jį, asmenybės teisių visumos apsauga. Asmens teisės į privatumą turinį sudaro savarankiški, tarpusavyje susiję privataus gyvenimo požymiai: fizinis, komunikacinis, teritorinis ir informacinis privatumas. Europos žmogaus teisių teismas pateikė privataus gyvenimo sampratą ir jo turinį, o Lietuvos Respublikos Konstitucinis Teismas pažodžiui perėmė šio teismo doktriną, palikdami erdvės šios sąvokos interpretacijai.

---

[23] Peck prieš Jungtinę Karalystę, Application No. 44647/98. 2003.

[24] „*Lietuvos Respublikos Konstitucijos komentaras (I dalis)*“ (Vilnius: Teisės institutas, K. Jovaišo PĮ, 2000): 162.

[25] „Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21 d. nutarimas Nr. 90-2662 „Dėl Lietuvos Respublikos Aukščiausiosios tarybos 1991m. sausio 31 d. nutarimo „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase” atitikimo Lietuvos Respublikos Konstitucijai“, LRKT, žiūrėta 2020 m. lapkričio 1 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta363.

[26] „Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas dėl Lietuvos Respublikos pataisos darbų kodekso 41 straipsnio 2 dalies (1997 m. liepos 2 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai“, LRKT, Žiūrėta 2020 m. lapkričio 1 d., http://www.lrkt.lt/dokumentai/2003/n030324.htm.

[27] Liudvika Meškauskaitė, Mindaugas Lankauskas, „Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos žmogaus teisių teismo bei Lietuvos teismų praktikos kontekste“, *Teisės problemo*s 1, 91 (2016): 56.

1.2. Teisės į privatumą ribos

Žmogaus teisių apsaugos šaltiniuose asmens privatumo sauga įtvirtinta kaip pagrindinė, fundamentali žmogaus teisė, tačiau ji nėra absoliuti. Šalys, kuriose savo jurisprudencijoje yra įtvirtinusios (ratifikavusios, integravusios) EŽTK, turi teisę imtis veiksmų, siekiant riboti asmens teisę į privatų gyvenimą, kai tai atitinka Konvencijos 8 str. 2 d. nustatytas sąlygas. Pažymėtina, kad teisėtų apribojimai atvejai turi būti numatyti įstatymu, taikomi pagrįstai, proporcingai siekiamam tikslui, siekiant valstybės teisėtų tikslų. Danutės Jočienės ir Kęstučio Čilinsko[28] teigimu, EŽTT praktikoje griežtai laikomasi šio teisėtumo, pagrįstumo ir proporcingumo principų.

EŽTK 8 str. 2 d.[29] reglamentuojama, kada galima pažeisti teisę į privatų gyvenimą, o kada ne. Vadinasi, teisė į privatų gyvenimą nėra absoliuti, šiai teisei galioja ribojimo sąlygos, kuomet reikalinga ginti viešąjį interesą, šalies ir/ar visuomenės saugumą, sveikatą, moralę ir vertybes, ekonominę gerovę, siekiant užtikrinti viešąją tvarką ir kt. Nors EŽTK 8 str. 2 d. numatyta asmens apsauga nuo valstybės pareigūnų kišimosi, tačiau EŽTT ne kartą akcentavo pozityvią valstybės pareigą užtikrinant privataus gyvenimo apsaugą. Byloje X ir Y prieš Nyderlandus[30] EŽTT pripažino, kad kartu su negatyvia pareiga – susilaikyti nuo kišimosi į privatų gyvenimą, yra taip pat ir valstybės pozityvus įsipareigojimas, kuris kyla iš privataus gyvenimo gerbimo principo, imantis priemonių, skirtų užtikrinti privataus gyvenimo gerbimą santykiuose tarp žmonių. Valstybės pačios pasirenka priemones, kuriomis siekia įgyvendinti pozityviuosius įsipareigojimus, užtikrinti pagarbą asmens privačiam gyvenimui, asmenų tarpusavių santykius.

Pažymėtina, kad ribojimo pagrindų sąrašas yra baigtinis – jokiais kitais pagrindais teisė į privatumą negali būti suvaržoma.

Remiantis LR Konstitucinio Teismo 2002 m. rugsėjo 19 d.[31] ir 2002 m. spalio 23 d.[32] nutarimais, žmogaus teisė į privatumą nėra absoliuti, ji turi ribojimo sąlygas. Remiantis LR Konstitucija, žmogaus teisė į privatumą ribojama keliais atvejais, kai pasitelkiamas įstatymas, siekiant apsaugoti kitų visuomenės narių laisvę ir teises, kitas šiame pagrindiniame šalies teisės akte įtvirtintas vertybes ir

[28] Danutė Jočienė, Kęstutis Čilinskas, „*Žmogaus teisių apsaugos problemos tarptautinėje ir Lietuvos Respublikos teisėje*“ (Vilnius: UAB „Petro ofsetas”, 2004): 74.
[29] „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
[30] X ir Y prieš Nyderlandus, Application No. 8978/80. 1985.
[31] „Lietuvos Respublikos Konstitucinio Teismo nutarimas „Dėl Telekomunikacijų, Operatyvinės veiklos įstatymų ir Baudžiamojo proceso kodekso“, LRKT, Žiūrėta 2020 m. lapkričio 1 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta309/content.
[32] „Lietuvos Respublikos Konstitucinio Teismo nutarimas „Dėl viešojo asmens privataus gyvenimo apsaugos ir žurnalisto teisės neatskleisti informacijos šaltinio“, LRKT, Žiūrėta 2020 m. lapkričio 1 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta311/content.

ginamus tikslus. Šie žmogaus į teisės į privatumą ribojimai nereiškia, kad įstatymu paneigiama žmogaus teisių ir laisvių prigimtis, tačiau LR Konstitucijoje įtvirtinto proporcingumo principo privalu laikytis.

LR CK 2.23 str. nustatyta, kad pažeisti asmens privatus gyvenimą negalima, kaip ir negalima skelbti informaciją apie kito asmens privatų gyvenimą, tam reikalingas asmens sutikimas. Asmeniui mirus, tokio pobūdžio sutikimą gali duoti artimieji. Taip pat LR CK 2.23 str. įtvirtinta, kad patekimas į kito asmens gyvenamąją vietą, jam priklausančią privačią teritoriją, šio asmens stebėjimas, pažeidžiant teisės aktus, turto krata, pokalbių ar susirašinėjimų skaitymas, rinkimas, dalijimasis su kitais apie kito asmens sveikatos būklę, yra ne tik šio asmens konfidencialumo pažeidimas, tai – privataus gyvenimo pažeidimas.

Apibendrinant galima teigti, kad asmens teisė į privatumą nėra absoliuti ir, remiantis tarptautiniais ir nacionaliniai teisės aktais, valstybinės institucijos neturi teisės riboti asmenes teisės į privatų gyvenimą, išskyrus atvejus, įtvirtintus EŽTK 8 str. 2 d., bei įstatymų nustatyta tvarka, siekiant užtikrinti valstybės saugumą, visuomenės sveikatos apsaugą, ginant šalies ekonominės gerovės interesus, užkertant kelią viešosios tvarkos pažeidimams ir nusikaltimams, ginant asmenų teisių ir laisvių visetą.

1.3. Asmens privatumo užtikrinimas

Kiekvienas asmuo savo privatumą suvokia ir supranta skirtingai, taip pat asmenys sprendžia, kurios gyvenimo detalės yra, pagal juos, privačios, o kurios ne. Kaip teigia Alvydas Pumputis ir kt.[33] asmens teisė į privatumą gali būti ginama tuomet, kai jo privatus gyvenimas bus pažeistas nesant jo sutikimui, kai bus pažeistos to asmens privataus gyvenimo apsaugos ribos. Anot Danutės Jočienės ir Kęstučio Čilinsko[34], asmens teisės į privatumą pažeisti negalima jokiomis priemonėmis, išskyrus tuos atvejus, kurie įtvirtinti įstatymu, laikantis teisės viršenybės principo, siekiant užtikrinti demokratinės visuomenės principus.

LR Konstitucinis Teismas konstatavo, kad LR Konstitucijoje įtvirtinta pagarba žmogaus teisėms ir laisvėms, kurioms užtikrinamos įvairiomis teisinėmis, finansinėmis, ir organizacinėmis priemonėmis. Taip pat LR Konstitucijoje įtvirtinta, kad pilietis, siekdamas apginti savo teises ir laisves turi teisę kreiptis į teismą. Remiantis LR Konstitucinio Teismo 2000 m. birželio 30 d. nutartimi[35], asmenys, siekdami apginti savo prigimtines teises ir laisves turi teisę į teisminį šių laisvių ir teisių gynimą.

---

[33] Alvydas Pumputis ir kt., „*Kontitucingumas ir pilietinė visuomenė*“ (Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002): 223.

[34] Danutė Jočienė, Kęstutis Čilinskas, „*Žmogaus teisių apsaugos problemos tarptautinėje ir Lietuvos Respublikos teisėje*“ (Vilnius: UAB „Petro ofsetas”, 2004): 58.

[35] „LR Konstitucinio Teismo 2000 m. birželio 30 d. nutartis Nr. 30/98-13/99 „Dėl Lietuvos Respublikos žalos, padarytos neteisėtais kvotos, tardymo, prokuratūros ir teismo veiksmais, atlyginimo įstatymo 3 str. 1 d. ir 4 str. 1 d. 1 p. atitikimo LR Konstitucijai“, LRKT, žiūrėta 2020 m. rugsėjo 17 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta343/content.

Išnaudojus visas nacionalines žmogaus teisių į privataus gyvenimo gynimo priemones, laikantis nustatyto termino, asmuo turi teisę, vadovaujantis EŽTK nuostatomis, kreiptis į EŽTT. Asmenys, kurių teisės pažeidžiamos Lietuvos Respublikos jurisdikcijoje, turi teisę kreiptis į EŽTT. Šiame teisme privataus gyvenimo neliečiamumas ginamas vadovaujantis EŽTK.

Pažymėtina, kad ES narės pripažįsta Europos Sąjungos Teisingumo Teismo (toliau – ESTT) jurisdikciją, taigi žmogaus teisės, taip pat ir informacija apie privatų asmens gyvenimą, yra ginamos ESTT.

Siekiant užtikrinti asmenų privatumą internetiniuose portaluose, aktualus EŽTK 8 str., kur užtikrinamos asmens teisės į privatumą ir Konvencijos 10 str., kuriame saugomos asmens saviraiškos laisvė. Pažymėtina, kad valstybinės institucijos ir interneto svetainių tiekėjai negali priimti sprendimų ir valdyti asmens veiksmų, kurie susiję su jo privatumu internete. Valstybinės institucijos ir interneto svetainių tiekėjai gali garantuoti, kad jų teikiamos privatumo saugos priemonės ir paslaugos būtų efektyvios, tačiau pasirinkimo laisvė, kokias privatumo apsaugos priemones ir būdus rinktis, tenka pačiam asmeniui[36].

Apibendrinant galima teigti, kad pagrindinis žmogaus asmens teisės į privatumą gynimo būdas – teisė kreiptis į teismą. Nepavykus apginti teisės į privatų gyvenimą nacionalinio lygmens teismuose, laikantis nustatyto termino, asmuo turi teisę, vadovaujantis Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencijos nuostatomis, kreiptis į Europos žmogaus teisių teismą. Taip pat asmuo gali ginti savo teisę į privatų gyvenimą Europos Teisingumo Teisme.

[36] Jordan E. Segall, „Google Street View: Walking the Line of Privacy –Intrusion upon Seclusion and Publicity Given to Private Facts in the Digital Age“, *Pittsburgh Journal of Technology Law and Policy, 1,* 14 (2010): 26.

2. ASMENS PRIVATUMO SAUGOS TEISINIO REGULIAVIMO RAIDA IR PROBLEMINIAI ASPEKTAI

2.1. Asmens teisė į privatumą tarptautiniuose teisės aktuose

Teisės į privatų gyvenimą teisinio reguliavimo pradžia siejama su asmens teisės į privatų gyvenimą doktrina[37]. Privatumo koncepcijos pradžia laikoma XIX a. Jungtinėse Amerikos Valstijose, vėliau ji buvo vystoma tiek šioje, tiek kitose šalyse[38]. Asmens privatumo saugos reguliavimo pradžia yra XIX a. 8 – tasis dešimtmetis, kurį paskatino sparti informacinių technologijų pažanga, padažnėjusios diskusijos apie privatumą, nes asmens duomenys buvo pradėti tvarkyti kompiuteriuose.

Visuotinė žmogaus teisių deklaracija[39] – pirmasis tarptautinis teisės aktas, kuriame 1948 m. įtvirtinta asmens teisė į privatumą. Šios deklaracijos 12 str. nustatyta, kad niekas neturi teisės kištis į kitos žmogaus gyvenimą, pažeisti jų privatumo, buitį, negali kėsintis į jų garbę, reputaciją, susirašinėjimus. Asmens teisė į privatumą buvo vėliau reglamentuojama ir kitais teisės aktais, pvz., 1966 m. buvo priimta Jungtinių Tautų Tarptautinio pilietinių ir politinių teisių paktas[40] (17 str.) ir Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija[41] (8 str.).

Pirmasis nacionalinis duomenų apsaugos įstatymas buvo priimtas Heseno žemėje (Vokietijos administracinis vienetas)[42]. Vėliau nacionaliniai aktai buvo priimti ir kitose Šiaurės (Švedijoje – 1973 m.; Norvegijoje, Danijoje – 1978 m.; Islandijoje – 1981 m.) Suomijoje – 1987 m.), Vakarų (Vokietijos Federacijoje – 1977 m.; Prancūzijoje, Liuksemburge – 1978 m., Jungtinėje Karalystėje – 1984 m.), Centrinės (Austrijoje – 1978 m.) Europos šalyse, Jungtinėse Amerikos Valstijose (1974 m.), Kanadoje, Naujojoje Zelandijoje (1982 m.), Australijoje, Japonijoje (1988 m.). Taigi technologijų pažanga privataus gyvenimo doktrinai tapo asmens duomenų teisinės apsaugos reguliavimo ašimi[43]. Ankstyvasis asmens privatumo apsaugos teisės raidos etapas rodo, kad Europos valstybės siekė įgyvendinti tarptautinius susitarimus, todėl harmonizavo nacionalinius teisės aktus, reglamentuojančius duomenų

[37] Ilona Petraitytė, „*Asmens duomenų teisinės apsaugos principai*“, Daktaro disertacija. Socialiniai mokslai, teisė (01S). (Vilnius: Vilniaus universitetas, 2013): 39.
[38] Edita Žiobienė, „Informacijos apie privatų asmens gyvenimą apsauga“. *Konstitucinė jurisprudencija, 3* (2008): 141.
[39] „Visuotinė žmogaus teisių deklaracija“, LRS, Žiūrėta 2020 m. spalio 31 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.
[40] „Tarptautinio pilietinių ir politinių teisių paktas“, LRS, Žiūrėta 2020 m. spalio 31 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.174848.
[41] „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
[42] Ernst Oliver Wilhelm, „*A brief History of the General Data Protection Regulation*“, 2016, žiūrėta 2020 m. rugsėjo 17 d. <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>.
[43] Ilona Petraitytė, „*Asmens duomenų teisinės apsaugos principai*“, Daktaro disertacija. Socialiniai mokslai, teisė (01S). (Vilnius: Vilniaus universitetas, 2013): 40.

apsaugos teisę, Europoje. Dėtos ypatingos pastangos asmens privatumo saugos teisės sureguliavime sumažino fizinės valstybių sienos reikšmę.

Tikslinga nagrinėti ir susisteminti pagrindines teisines priemones, kurios taikomos siekiant užtikrinti asmens privatumo saugą.

1981 m. sausio 28 d. Europos Taryba priėmė Konvenciją Nr. 108 „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“[44]. Tai buvo pirmasis teisiškai įpareigojantis tarptautinis dokumentas, priimtas duomenų apsaugos srityje. Jo tikslas – užtikrinti, kad, tvarkant asmens duomenis automatizuotai, visų šalių teritorijose būtų gerbiamos kiekvieno asmens, nepaisant jo tautybės ir gyvenamosios vietos, teisės ir pagrindinės laisvės, o svarbiausia, jo teisė į privatų gyvenimą. Konvenciją keitė protokolas[45], kuriuo iš dalies keista Europos Tarybos konvencija, siekta išplėsti jos taikymo sritį, išplėsti duomenų apsaugą ir pagerinti jos veiksmingumą.

Teisė į privatų gyvenimą garantuoja EŽTK 8 str. 1 d., kur teigiama, kad „kiekvienas turi teisę į tai, kad būtų gerbiamas jo privatus ir šeimos gyvenimas, būsto neliečiamybė ir susirašinėjimo slaptumas“[46]. Ši teisė nėra absoliuti ir šie teisės į privatų gyvenimą ribojimai numatyti 8 str. 2 d. Apriboti asmens teisę į privatų gyvenimą gali valstybės institucijos, kai ši ribojimo galimybė yra nustatyta įstatymu. Taip pat tokio pobūdžio ribojimas yra būtinas demokratinėje visuomenėje, siekiant užtikrinti valstybės ir visuomenės saugumo interesu, rūpintis žmonių sveikatos ir kitų teisių apsauga.

Dar vienas svarbus tarptautinis teisės aktas, kuriame garantuojama asmens teisė į privatumą, informacijos saugą – Europos Sąjungos pagrindinių teisių chartija[47] (toliau – Chartija). Chartijos 7 str. įtvirtinta, kad visi turi teisę, kad jų gyvenimas (šeimyninis ar privatus) būtų gerbiamas, būstas neliečiamas, o informacijos perdavimas – slaptas. Chartijos 8 str. garantuojama teisė, kad asmens duomenys bus apsaugoti, tinkamai tvarkomi, naudojami pagal paskirtį (asmeniui sutikus) tik įstatymų nustatytais atvejais (panaši garantija įtvirtina ir LR Konstitucijoje). Kiekvienas asmuo gali susipažinti su tais duomenimis, kurie apie jį yra surinkti, su tikslu juos ištaisyti. Chartijos 52 str. 3 d. įtvirtinta, kad „Chartijoje nurodytų teisių, atitinkančių EŽTK garantuojamas teises, esmė ir taikymo sritis yra tokia,

[44] „Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu (ETS Nr. 108) su Europos Tarybos Ministrų Komiteto priimtomis pataisomis“, LRS, žiūrėta 2021 m. balandžio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.129872.

[45] „Protokolas, kuriuo iš dalies keičiama Europos Tarybos konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“, LRS, žiūrėta 2021 m. balandžio 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/d8e8a420c89811e9a56df936f065a619?jfwid=-a3k5bxsmf.

[46] „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.

[47] „Europos Sąjungos pagrindinių teisių chartija“, Eur-lex, , žiūrėta 2020 m. spalio 27 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

kaip nustatyta toje Konvencijoje“[48]. Ši nuostata reiškia, kad ES teisėje galima numatyti didesnę apsaugą. ES pozicija asmens duomenų apsaugos srityje turi būti stiprinama vykdant asmens privatumo saugos politiką visoje ES, įskaitant teisėsaugą ir nusikalstamumo prevenciją, taip pat tarptautinius santykius, ypač pasaulinėje visuomenėje, kuriai būdingi spartūs technologiniai pokyčiai.

Būtina paminėti taip pat Tarptautinį pilietinių ir politinių teisių paktą[49], kuris buvo priimtas LR Aukščiausiosios Tarybos 1991 m. kovo 12 d., dar iki Lietuvai priimant LR Konstituciją. Šio pakto 17 str. įtvirtinta, kad negalima kištis į kito asmens šeimyninį ir asmeninį gyvenimą, liesti ar įeiti į privačią nuosavybę, skaityti, tvarkyti ar dalytis susirašinėjimais, kėsintis į jų garbę, orumą. Taip pat kiekvienam yra garantuojama teisė į įstatymu nustatytą apsaugą. Kurt Herndl išreiškė asmeninę nuomonę[50], kad pakto 17 str. įvirtinta nuostata dėl teisės į privatumą yra nevienareikšmė ir, kad teisė į privatumą čia pateikiama kaip privatumo koncepcijos dalis.

Kitas svarbus teisės aktas, kuris saugo asmenes teisę į privatumą – Europos Parlamento ir Europos Tarybos direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB)“. Šios direktyvos 6 str., įtvirtinta, kad asmens duomenys turi būti „surinkti įvardintais, aiškiai apibrėžtais ir teisėtais tikslais, o po to tvarkomi su šiais tikslais suderintais būdais“[51]. Šios direktyvos 7 str. įtvirtinta, kad asmens duomenys gali būti tvarkomi tada, kuomet, kai duomenų subjektas duoda nedviprasmišką sutikimą tvarkyti jo duomenis.

2002 m. liepos 12 d. Europos Parlamentas ir Europos Taryba priėmė direktyvą 2002/58/EB[52], kuri buvo iš dalies pakeista direktyva 2009/136/EB, priimta 2009 m. lapkričio 25 d. Direktyvoje akcentuojamas opus duomenų saugojimo klausimas, kuris buvo ne kartą buvo nagrinėtas ESTT ir dėl kurio buvo priimta daugybė nutarimų, paskutinį kartą – 2020 m., aiškinant, kad ES įstatymai draudžia saugoti pranešimų srautą ir vietos duomenis. Šiuo metu svarstomas naujas Europos Parlamento ir Europos Tarybos reglamentas dėl pagarbos asmeniniam gyvenimui ir asmens duomenų apsaugos

[48] „Europos Sąjungos pagrindinių teisių chartija“, Eur-lex, , žiūrėta 2020 m. spalio 27 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

[49] „Tarptautinis pilietinių ir politinių teisių paktas“, LRS, žiūrėta 2021 m. vasario 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.174848,

[50] United Nations, „Individual opinion (dissenting) submitted by Mr. Kurt Herndl pursuant to rule 94, paragraph 3, of the rules of procedure of the Committee on Human Right“, 2005, žiūrėta 2021 m. vasario 2 d., https://www.ohchr.org/Documents/Publications/SDecisionsVol5en.pdf.

[51] „Europos Parlamentas ir Tarybos direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB)“, Eur-lex, žiūrėta 2020 m. lapkričio 1 d., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:LT:NOT.

[52] „2002 m. liepos 12 d. Europos Parlamento ir Tarybos direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje“, Eur-lex, žiūrėta 2020 m. lapkričio 1 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32002L0058.

elektroniniuose ryšiuose pasiūlymas, kuriuo bus panaikinta direktyva 2002/58/EB (reglamentas dėl privatumo ir elektroninių ryšių).

Dėl sparčių technologinių pokyčių, globalizacijos raiškos, duomenų apsaugos taisykles reikėjo reformuoti. 2012 m. Europos Komisija pasiūlė reformuoti duomenų apsaugą[53]. Duomenų apsaugos direktyvą panaikino ir reformavo 2016 m. balandžio 27 d. Europos Parlamento ir Europos Tarybos priimtas reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis (toliau – Bendrasis duomenų apsaugos reglamentas arba BDAR). Naujasis reglamentas taikomas visose ES valstybėse narėse nuo 2018 m. gegužės 25 d. Pažymėtina, kad BDAR yra reikšmingas ne tik asmenų duomenų apsaugai, tačiau šis teisės aktas svarbus ir Europos ekonominei erdvei (EEE), nes reglamentas tęsia siekį „užbaigti kurti laisvės, saugumo ir teisingumo erdvę ir ekonominę sąjungą, skatinti ekonominę ir socialinę pažangą, stiprinti valstybių narių ekonomiką ir siekti jų ekonomikos konvergencijos vidaus rinkoje ir fizinių asmenų gerovės“[54]. Remiantis BDAR, piliečių turimos teisės apima: aiškus ir patvirtinantis sutikimas, kad jų duomenys būtų tvarkomi, ir teisė gauti aiškią ir suprantamą informaciją apie juos; teisė būti pamirštam: pilietis gali prašyti ištrinti jo duomenis; teisė perduoti duomenis kitam paslaugų teikėjui (pvz., perėjus iš vieno socialinio tinklo į kitą); ir teisė žinoti, kada privatumo sauga buvo pažeista. Naujosios taisyklės taikomos visoms ES veikiančioms įmonėms, net ir toms, kurios įsikūrusios už jos ribų. Be to, įmonėms, kurios pažeidžia taisykles, gali būti taikomos priemonės, tokios kaip įspėjimai arba baudos.

2016 m. balandžio 27 d. Europos Parlamentas ir Europos Taryba priėmė direktyvą (ES) 2016/680, kuriuo panaikinamas Europos Tarybos pamatinis sprendimas 2008/977/TVR. Direktyva užtikrina, kad aukų, liudininkų ir įtariamų nusikaltimais asmenų duomenys būtų tinkamai apsaugoti, ir palengvintų tarpvalstybinį bendradarbiavimą kovojant su nusikalstamumu ir terorizmu.

2018 m. spalio 23 d. Europos Parlamento ir Europos Tarybos priimtas reglamentas (ES) 2018/1725[55] dėl fizinių asmenų apsaugos tvarkant asmens duomenis Sąjungos institucijose, įstaigose, biuruose ir agentūrose ir dėl nemokamo tokių duomenų judėjimo, panaikino reglamentą (EB) Nr. 45/2001 ir sprendimą Nr. 1247/2002/EB.

---

[53] Europos Komisija. 2012 m. sausio 25 d. Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas), KOM(2012) 11 galutinis, Briuselis.

[54] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4, p. 1–88.

[55] „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“, Eur-lex, žiūrėta 2021 m. vasario 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX%3A32018R1725.

Pateikiami pagrindiniai ES tarptautiniai susitarimai dėl duomenų perdavimo:

- Duomenų perdavimas komerciniais tikslais. Remiantis BDAR 45 str., Europos Komisija turi įgaliojimus nustatyti, ar už ES ribų esanti šalis užtikrina pakankamą duomenų apsaugos lygį, siekiant laikytis tarptautinių įsipareigojimų, kuriuos ji prisiėmė. Europos Parlamentas priėmė keletą rezoliucijų, kuriomis išreiškė susirūpinimą dėl transatlantinių duomenų srautų. Visų pirma, manoma, kad ES ir JAV „privatumo skydas“ neužtikrina tinkamo apsaugos lygio, kurio siekiama ES teisės aktais, o nacionaliniai teismai ne kartą pripažino ESTT sprendimus negaliojančiais (pvz., ESTT sprendimas Nr. 2000/520, taip vadinamasis „saugaus uosto“ sprendimas[56]. Europos Komisija konstatavo, kad JAV neužtikrina tinkamą apsaugos lygį. Gavęs Airijos Aukštojo Teismo prejudicinį klausimą, 2015 m. prieš tai priimtą sprendimą, kad JAV užtikriną tinkamą apsaugos lygį, ESTT pripažino negaliojančiu).
- ES – JAV „privatumo skydas“[57]. Europos Parlamentas dalyvavo tvirtinant JAV ir ES susitarimus dėl asmeninės informacijos apsaugos, susijusios su nusikalstamų veikų prevencija, tyrimu, nustatymu ir patraukimu už jas baudžiamojon atsakomybėn, dar vadinamą „Privatumo skydas“. Šio susitarimo tikslas yra užtikrinti aukšto lygio asmeninės informacijos, perduotos vykdant susitarimą dėl transatlantinio bendradarbiavimo teisėsaugos tikslais, apsaugą, kovojant su terorizmu ir organizuotu nusikalstamumu.
- ES – JAV, ES – Australijos bei ES – Kanados susitarimai dėl keleivių duomenų įrašo (PNR)[58]. ES pasirašė dvišalius keleivių duomenų įrašo (PNR) susitarimus su JAV, Australija ir Kanada. PNR duomenys apima keleivių pateiktą informaciją užsakant ar registruojantis skrydžius, oro vežėjų komerciniais tikslais surinktus duomenis. Teisėsaugos institucijos PNR duomenis gali naudoti kovai su sunkiais nusikaltimais ir terorizmu.
- ES ir JAV susitarimas dėl finansinių mokėjimų pranešimų duomenų perdavimo[59]. ES pasirašė dvišalį susitarimą su JAV dėl finansinių mokėjimų pranešimų duomenų tvarkymo ir perdavimo iš ES – JAV pagal teroristų finansavimo paieškos programą.

[56] Europos Sąjungos Teisingumo Teismas, „Metinis pranešimas 2015. Teisminė veikla. Teisingumo Teismo, Bendrojo Teismo ir Tarnautojų teismo veiklos apžvalga“ (Liuksemburgas, 2016), žiūrėta 2021 m. vasario 2 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2016-04/rapport_annuel_2015_activite_judiciaire_lt.pdf.

[57] „ES ir JAV „Privatumo skydo“ gairės“, žiūrėta 2021 m. vasario 2 d., https://ec.europa.eu/newsroom/document.cfm?doc_id=47770.

[58] „Europos Parlamento rezoliucija dėl derybų dėl susitarimų dėl keleivio duomenų įrašo (PNR) su JAV, Australija ir Kanada pradžios“, žiūrėta 2021 m. vasario 2 d., https://www.europarl.europa.eu/doceo/document/B-7-2010-0244_LT.html.

[59] „Europos Sąjungos ir Jungtinių Amerikos Valstijų susitarimas dėl finansinių mokėjimų pranešimų duomenų perdavimo“, žiūrėta 2021 m. vasario 2 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:jl0039/

- ES duomenų apsaugos priežiūros institucijos. Europos duomenų apsaugos priežiūros pareigūnas (EDAPP) yra įgaliotas užtikrinti, kad ES institucijos ir įstaigos vykdytų savo įsipareigojimus, susijusius su duomenų apsauga[60].

Teisės aktų įgyvendinimo stebėsenai ir įgyvendinimui, reikalinga institucinė sąranga. Prieš įsigaliojant Lisabonos sutarčiai, teisės aktai dėl duomenų apsaugos laisvės, saugumo ir teisingumo erdvėje (toliau – LSTE) buvo skirstomi į pirmąjį ramstį (duomenų apsauga privatiems ir komerciniams tikslams) ir trečiasis ramstis (duomenų apsauga teisėsaugos tikslais tarpvyriausybiniu lygmeniu). Dėl skirstymo į ramsčius asmenes privatumo saugos užtikrinimo procesai vyko remiantis skirtingomis taisyklėmis. Ramsčiais paremta struktūra išnyko įsigaliojus Lisabonos sutarčiai, kuri suteikė tvirtesnį pagrindą kuriant aiškesnę ir veiksmingesnę asmens privatumo saugos sistemą, tuo pačiu suteikiant naujas galias Europos Parlamentui. Sutarties dėl Europos Sąjungos veikimo 16 str. numatyta, kad Europos Parlamentas ir Europos Taryba nustato taisykles, susijusias su asmenų apsauga tvarkant šiuos duomenis ES institucijose, įstaigose, tarnybose ir agentūrose bei valstybėse narėse vykdant veiklą, kuriai taikoma ES teisė[61]. Dabar Europos Parlamentas daugiausia dėmesio skiria ES duomenų apsaugos teisės aktų įgyvendinimo stebėsenai, dirbtinio intelekto duomenų apsaugos aspektams ir skaitmeninių paslaugų įstatymui bei kitiems būsimiems Europos Komisijos pasiūlymams, kurie gali turėti įtakos duomenų apsaugai.

Europos duomenų apsaugos valdyba (EDAV), buvusi 29 straipsnio darbo grupė – nepriklausoma ES įstaiga, kuri vienija priežiūros institucijas visame ES. EDAV padeda užtikrinti nuoseklų duomenų apsaugos taisyklių taikymą visoje ES ir skatina duomenų apsaugos institucijų bendradarbiavimą[62].

Apibendrinant galima teigti, kad asmens teisė į privatumą tarptautiniuose teisės aktuose reguliuojama pakankamai. Asmens teisė į privatų gyvenimą, asmenų duomenų apsaugą garantuoja Konvencija Nr. 108 „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“, Europos žmogaus teisių konvencija, Europos Sąjungos pagrindinių teisių chartija, Tarptautinis pilietinių ir politinių teisių paktas. Europos Sąjungos lygmeniu priimta eilė direktyvų, tačiau pagrindinė jų – Bendrasis duomenų apsaugos reglamentas, kuris taikomas visose ES valstybėse narėse nuo 2018 m. gegužės 25 d. Bendrasis duomenų apsaugos reglamentas užtikrina piliečių teises: dėl aiškaus sutikimo tvarkyti jų duomenis, dėl teisės būti pamirštam, dėl teisės perduoti duomenis kitam paslaugų tiekėjui, dėl

[60] Europos Sąjunga, „Europos duomenų apsaugos priežiūros pareigūnas (EDAPP). Europos duomenų apsaugos priežiūros pareigūno veikla“, žiūrėta 2021 m. vasario 2 d., https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_lt.

[61] Europos Parlamentas, „Fact Sheets on the European Union – 2021“, žiūrėta 2021 m. vasario 2 d., https://www.europarl.europa.eu/ftu/pdf/en/FTU_4.2.8.pdf#page=3.

[62] European Data Protection Board, „Apie EDAV“, žiūrėta 2021 m. vasario 2 d., https://edpb.europa.eu/about-edpb/about-edpb_lt.

teisės žinoti, kada privatumo sauga buvo pažeista. Naujosios taisyklės taikomos visoms ES veikiančioms įmonėms, net ir toms, kurios įsikūrusios už jos ribų. Be to, įmonėms, kurios pažeidžia taisykles taikomos priemonės: įspėjimai arba baudos.

2.2. Asmens teisės į privatumą nacionaliniuose teisės aktuose

LR Konstitucijos 22 str. 1 d. įtvirtinta asmens teisė į privatų gyvenimą. Šioje nuostatoje įtvirtintas bendrasis principas, kad žmogaus privatus gyvenimas yra neliečiamas. LR Konstitucijos 22 str. 2 d. įvardinti privataus gyvenimo objektai, kurie turėtų būti neliečiami: asmens susirašinėjimas, pokalbiai telefonu, telegrafo pranešimai ir kitoks susižinojimas. Edita Žiobienė[63] paaiškina, ką reiškia „kitoks susižinojimas“ teigdama, kad ši sąvoka apima visas greitai evoliucionuojančias informacijos priemones (pvz., internetas, elektroninis paštas ir kt.). LR Konstitucijos 22 str. 3 d. įtvirtinta, kad „informacija apie privatų asmens gyvenimą gali būti renkama tik motyvuotu teismo sprendimu ir tik pagal įstatymą“[64]. To paties straipsnio 4 d. „saugo asmens garbę ir orumą, kuomet įstatymas ir teismas saugo, kad niekas nepatirtų savavališko ar neteisėto kišimosi į jo asmeninį ir šeimyninį gyvenimą, kėsinimosi į jo garbę ir orumą“[65].

Lietuvoje asmens privatumo saugos apsauga buvo susirūpinta tik atgavus nepriklausomybę, kai 1990 m. kovo 11 d. buvo priimtas Lietuvos Respublikos laikinasis pagrindinis įstatymas (toliau – LR laikinasis pagrindinis įstatymas). Šio įstatymo 35 str. įtvirtinta, kad piliečių asmeninis gyvenimas, jų susirašinėjimas, telefoniniai pokalbiai, telegrafiniai pranešimai yra slapti, ir šiuos duomenis saugo įstatymas. 1992 m. įsigaliojusios LR Konstitucijos 22 str. 1 d. įtvirtinta žmogaus teisė į privatumą, šio gyvenimo neliečiamumą, o 3 d. – informaciją apie asmens privatų gyvenimą renkamą tik pagal įstatymą, esant motyvuotam teismo sprendimui. 1996 m. birželio 11 d. buvo priimtas Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (toliau – LR Asmens duomenų teisinės apsaugos įstatymas), kuris laikomas pirmuoju specialiuoju nacionaliniu teisės aktu. Teisės aktas buvo skirtas reguliuoti asmens duomenų tvarkymą šalyje, įtvirtinti asmenuos duomenų rinkimo, kaupimo, apdorojimo, saugojimo, naudojimo ir teikimo reikalavimai. LR asmens duomenų teisinės apsaugos įstatymas reguliavo gana siaurą visuomeninių santykių sritį, tačiau informacijos tvarkymo reikalavimai buvo griežti. Spartus (informacinių) technologijų sklaida ir raida nulėmė, kad asmenų duomenis informacinėse sistemose pradėjo tvarkyti ne tik valstybė, bet ir privatūs asmenys. Atsižvelgiant į šiuos pokyčius, 1998 m. priimtos

[63] Edita Žiobienė, „Aktualios konstitucinės teisės į privatų gyvenimą apsaugos problemos“, *Jurisprudencija, 64* (2005): 124.
[64] „Lietuvos Respublikos Konstitucija“, LRS, žiūrėta 2021 m. vasario 2 d., https://www.lrs.lt/home/Konstitucija/Konstitucija.htm.
[65] Ten pat.

LR Asmens duomenų teisinės apsaugos įstatymo pataisos, kurios praplėtė įstatymo taikymo sritis, supaprastino informacijos asmenų duomenų tvarkymo sąlygas. Lietuvai siekiant narystės ES, reikėjo keisti LR Asmens duomenų teisinės apsaugos įstatymo redakciją nauja. Šis nacionalinis teisės aktas buvo suderintas su 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. LR asmens duomenų teisinės apsaugos įstatymo pakeitimo įstatyme įvardytas siekis ginti žmogaus privataus gyvenimo neliečiamumo teisę ryšium su asmens duomenų tvarkymu ir sudaryti sąlygas laisvam asmens duomenų judėjimui. Taip pat išplėsta nacionalinio teisės akto apsaugos sritis, priskirti visi asmens duomenys, kurie tvarkomi, nustatyti teisėto asmens duomenų tvarkymo pagrindai, duomenų subjektų teisės ir duomenų valdytojų pareigos, įstatymo vykdymą prižiūrinčios institucijos. Pažymėtina, kad LR asmens duomenų teisinės apsaugos įstatymas iki 2018 metų buvo keičiamas daugelį kartų. Paskutinė įstatymo naujo redakcija priimta 2018 m. birželio 30 d.

Asmens teisę į privatumą saugo taip pat ir LR visuomenės informavimo įstatymas. LR visuomenės informavimo įstatymo 19 str. 9 d.[66] įtvirtinta asmens teisė ginti informaciją apie privataus gyvenimo neliečiamumą ikiteisminėje institucijose: pranešant žurnalistų etikos inspektoriui, Lietuvos radijo ir televizijos komisijai. Pažymėtina, kad šis įstatymas taikomas, jeigu jis neprieštarauja LR CK 1.3 str. 2 d., kurioje numatyta, kad asmens sutikimo nereikia, kai asmuo fotografuojamas viešoje vietoje, tačiau demonstruoti draudžiama, jeigu tai žemina asmens garbe, orumą, dalykinę reputaciją.

Dar vienas nacionalinis teisės aktas, saugas asmens teisę į privatumą, – Lietuvos Respublikos baudžiamasis kodeksas[67] (toliau – LR BK). LR BK XXIV skyriuje numatyta baudžiamoji atsakomybė už pažeidimus susijusius su asmens privataus gyvenimo pažeidimais. Kaip teigia Liudvika Meškauskaitė ir Mindaugas Lanksauskas, „baudžiamosios atsakomybės nustatymas padeda siekti EŽTK numatytų tikslų, t. y. užtikrinti, kad būtų gerbiamas privatus asmenų gyvenimas. Šiuo atveju svarbu pažymėti, jog privatumo apsaugos įtvirtinimas vien įstatymais dar nereiškia, jog teisė į privatumą yra efektyviai ginama. Nesant galimybės teismuose efektyviai ginti šios teisės, gali būti konstatuotas EŽTK pažeidimas“ [68].

Vystantis elektroninei komercijai, augant teikiamų elektroninių, finansinių ir viešųjų paslaugų apimtis, tapo svarbu užtikrinti, kad asmens tapatybė būtų identifikuojama saugiai. Šiam tikslui užtikrinti

[66] „Lietuvos Respublikos visuomenės informavimo įstatymas“, TAR, žiūrėta 2020 m. rugsėjo 17 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr.
[67] „Lietuvos Respublikos baudžiamasis kodeksas“, TAR, Žiūrėta 2020 m. lapkričio 1 d.,
[68] Liudvika Meškauskaitė, Mindaugas Lankauskas, „Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos žmogaus teisių teismo bei Lietuvos teismų praktikos kontekste“, *Teisės problemo*s 1, 91 (2016): 59.

buvo parengtas LR elektroninių ryšių įstatymas[69]. Šis įstatymas skirtas reglamentuoti duomenų, generuojamų arba tvarkomų teikiant viešąsias elektroninių ryšių paslaugas, tvarkymą ir privatumo apsaugą. Taip pat teisės akte reglamentuojama kaip institucijos, teikiančios elektroninių ryšių paslaugas, turi tvarkyti asmens duomenis. Šio įstatymo 69 str. 1 d. įtvirtinta, kad siekiat teikti elektroninių ryšių paslaugas, siunčiant pranešimus el. paštu ar trumposiomis žinutėmis, tiesioginės rinkodaros tikslu, būtina gauti išankstinį asmens ar registruoto naudotojo sutikimą. Jeigu šios nuostatos nesilaikoma, teigiama, kad įmonė pažeidė įstatymą. Taip pat įstatyme atkreipiamas dėmesys į grėsmes, kurios kyla asmens privatumo saugai.

Asmens teisė į privatumą užtikrinama dar vienu LR teisės aktu – LR advokatūros įstatymu[70]. Šiame įstatyme įtvirtinti specifiniai asmens duomenų tvarkymo ypatumai, kurie siejami su advokatų pareigomis ir veiklos taisyklėmis, kaip elgtis su asmeniu ir jam patikėtais asmens duomenimis. Šio įstatymo 9 str. įtvirtintos advokato pareigos, ir akcentuojama, kad vykdant veiklą jis privalo laikytis duotos advokato priesaikos, įstatymų, saugoti jam patikėtą informaciją, jos neatskleisti. Asmuo, dirbdamas su advokatu, taip pat privalo laikytis konfidencialumo principo ir negali trečiosioms šalims (asmenims) atskleisti informacijos, jam suteiktos darbo su advokatu metu.

Taip pat skiriami šie teisės aktai susiję su asmens teisės į privatumą nacionaliniuose teisės aktuose: LR pacientų teisių ir žalos sveikatai atlyginimo įstatymas[71] ir LR nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas[72]. LR pacientų teisių ir žalos sveikatai atlyginimo įstatymo 10 str. įtvirtinta, kad „pacientų privatus gyvenimas yra neliečiamas, bei, kad visa informacija apie paciento sveikatos būklę, diagnozę, prognozes ir gydymą, taip pat visa kita asmeninio pobūdžio informacija apie pacientą turi būti laikoma konfidencialia net ir po paciento mirties“ [73]. LR nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas nustato, kad „visuomenės informavimo priemonėse draudžiama skleisti neigiamą poveikį nepilnamečių vystymuisi darančią informaciją, susijusią su nepilnamečio asmens duomenimis, pagal kuriuos galima nustatyti jo asmens tapatybę“[74].

---

[69] „Lietuvos Respublikos elektroninių ryšių įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/RKktjkmTCK.

[70] „Lietuvos Respublikos advokatūros įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.229789?jf.

[71] „Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.31932?jfwid=32wf94v5.

[72] „Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.183129/OEFZHiiLcf.

[73] „Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.31932?jfwid=32wf94v5.

[74] Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.183129/OEFZHiiLcf.

Apibendrinant galima teigti, kad Lietuvos Respublikoje kuriami ir tobulinami asmens teisės į privatumą teisinio reguliavimo pagrindai. Nacionaliniai teisės aktai reguliuojantys asmens teisės į privatumą apima įvairias gyvenimo sritis, įvairaus amžiaus grupių asmenis, todėl galima daryti išvadą, kad teisinis reglamentavimas yra pakankamas. Atsižvelgiant į besikeičiančią situaciją visuomenėje, technologinę pažangą, teisės aktai turi būti peržiūrimi, keičiami ir adaptuojami.

3. ASMENS PRIVATUMO SAUGA SOCIALINIUOSE TINKLUOSE

3.1. Socialinio tinklo samprata ir asmens privatumo sauga jame

Internete yra daugybė socialinių svetainių (tinklų), kuriose žmonės, turintys bendrų interesų, gali dalytis mintimis, idėjomis, planais ar kalbėtis apie (gyvenimo) įvykius. Anot Dare Abel Lamidi ir kt. [75], žiniatinklio vartotojai kuria internetines bendruomenes, socialinius tinklus, kurie gali apimti neribotą temų skaičių. Socialinis tinklas gali jungti draugus, gimines, užtikrinti finansinių mainų, dalijimosi religiniais įsitikinimais ar praktiškai bet kokio tipo bendrais interesais galimybę. Iki socialinių tinklų įsitvirtinimo, vienpusiam informacijos transliavimui ir sklaidai pakako turėti internetą. Šiandien tokie socialiniai tinklai kaip „Facebook“ ir „Twitter“ skatina naujas socialinės sąveikos, dialogo, informacijos mainų ir bendradarbiavimo formas. Dėl paprastų pašnekesių ar naujienų skleidimo, išreiškiant švelnų humorą ar atliekant rimtus tyrimus, socialinius tinklus dėl įvairių priežasčių dabar įgalina įvairios vartotojų bendruomenės. Kaip teigia Simeon Edosomwan ir kt.[76], socialiniai tinklai („Facebook“, „Twitter“, „LinkedIn“ ir daugelis kitų) tapo tikrai reikšmingomis žmonijos bendravimo ir sąveikos priemonėmis, kas turėti didelį poveikį žmonių santykiams ir ryšiams.

Remiantis Dare Abel Lamidi ir kt.[77], socialiniai tinklai – tai asmenų ir/ar organizacijų visuma, susietų vienu ar keliais asmenimis, tokiais kaip draugai, bendruomenė ir kt. Dahan Boyd ir Nicole Ellison[78] socialinių tinklų svetaines apibūdina kaip sistemas, leidžiančias asmenims: susikurti viešą ar pusiau viešą profilį ribotoje sistemoje; nuspręsti (sudaryti „draugų“ sąrašą), su kuriais vartotojai, turės ryšį; peržiūrėti savo rate turimų vartotojų sukurtų ryšių sąrašą. Taip pat pažymima, kad šie tinklai skiriasi pagal funkcijas ir narystės pobūdį. Kai kuriuose tinkluose leidžiama dalytis nuotraukomis/vaizdo įrašais, kituose – tinklaraščiais ir asmeniniais pranešimais. Anot Simeon Edosomwan ir kt.[79], iš dalies tinklaraščiai taip pat buvo laikomi socialinių tinklų forma, nes jie palaiko ir skatina socialinių ryšių formavimąsi. Tinklaraščiai, pokalbių svetainės, tiesioginės pranešimų priemonės, pranešimų lentos ir

[75] Lamidi, Dare Abel, Gana Makun, Alafiatayo, Benjamin, „Use of Social Media in Information Dissemination“, 2014, žiūrėta 2021 m. vasario 1 d., https://www.researchgate.net/publication/319230692_Use_of_Social_Media_in_Information_Dissemination.
[76] Simeon Edosomwan, Sitalaskshmi Prakasan, Doriane Kouame, Jonelle Watson, Tom Seymour, „The History of Social Media and its Impact on Business“. *The Journal of Applied Management and Entrepreneurship, 16* (2011): 4.
[77] Lamidi, Dare Abel, Gana Makun, Alafiatayo, Benjamin, „Use of Social Media in Information Dissemination“, 2014, žiūrėta 2021 m. vasario 1 d., https://www.researchgate.net/publication/319230692_Use_of_Social_Media_in_Information_Dissemination.
[78] Dahan Boyd, Nicole Ellison, „Social network sites: definition, history, and scholarship“. Journal of computer-mediated communication, 13 (2007), žiūrėta 2021 m. vasario 1 d., https://academic.oup.com/jcmc/article/13/1/210/4583062.
[79] Simeon, Edosomwan, Sitalaskshmi, Prakasan, Doriane, Kouame, Jonelle, Watson, Tom, Seymour, „The History of Social Media and its Impact on Business“. *The Journal of Applied Management and Entrepreneurship, 16* (2011): 4.

socialinių žymių ženklai yra „Web 2.0“ technologijos dalis, kuri naudojama palengvinant narių sąveiką, todėl vadinama socialinių tinklų įrankiu.

Kaip teigia Nicolae Sfetcu[80], socialiniai tinklai yra socialinė struktūra, leidžianti vartotojui bendrauti ir bendradarbiauti su kitais vartotojais, įskaitant galimybę naršyti, ieškoti, kviesti draugus prisijungti ir bendrauti su visu pasauliu. Socialinė programinė įranga „Web 2.0“ pasaulyje ne tik pagerina naudojimąsi socialiniais tinklais, o socialinių tinklų svetainės yra naudingos norint suaktyvinti vartotojų sąveiką

Socialiniams tinklams būdingi tam tikri bruožai. Visų pirma, anot Ingos Malinauskaitės[81], socialiniai tinklai yra tokia vieta, kur susitinka šių tinklų vartotojai (bendruomenės nariai) ir šių (socialinių ir interneto) tinklų teikėjai. Antra, socialiniuose tinkluose vykdytą veiklą galima atkurti ir peržiūrėti. Trečia, socialiniams tinklams būdinga monetizacija, komercija, pelno maksimizavimas per įvairias komunikacijos, prekybos priemones. Paskutinis bruožas tas, kad socialiniai tinklai yra prieinami beveik visame pasaulyje, t.y. jie veikia peržengdami nacionalinių šalių ribas.

Mokslinėje literatūroje nėra vieningos socialinio tinklų klasifikacijos. Vieni autoriai socialinius tinklus nagrinėja pagal jų tuometinį populiarumą[82], kiti pagal vartotojų skaičių[83]. Yra šaltinių, kurie socialinius tinklus grupuoja pagal jų prieinamumą[84] arba tipą[85].

Michaeol Beye ir kt.[86] grupuoja socialinius tinklus į ryšių ir turinio socialinius tinklus:

- socialinių ryšių tinklai. Šio tipo tinkluose daugiau dėmesio skiriama naudotojų ryšiams. Ryšiai formuojami sujungiant vartotojus ir pateikiant jų socialinių kontaktų sąrašą. Socialinių ryšių tinklai – tai pažinčių svetainės, verslo, socialinių santykių palaikymo, bendravimo socialiniai tinklai:
    - pažinčių svetainės. Pažinčių svetainės yra svetainės, kurių tikslas – padėti vartotojams surasti draugą, partnerį, t.y. antrą pusę. Kiekvienas vartotojas turi turėti profilį. Pranešimai, kuriais keičiasi vartotojai yra privatūs, neretai intymaus pobūdžio.

[80] Nicolae Sfetcu, „Web 2.0 / Social media / Social networks“. 2017, žiūrėta 2021 m. vasario 1 d., https://www.researchgate.net/publication/338345786_Web_20_Social_Media_Social_Networks.
[81] Inga Malinauskaitė, „Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė“, *Social Transformations in Contemporary Society* 3, (2015): 122.
[82] Mary Gormandy, White. „What Types of Social Networks Exist?“. 2021, žiūrėta 2021 m. vasario 7 d., https://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist.
[83] ClickZ. 2021, žiūrėta 2021 m. vasario 7 d., https://www.clickz.com/type/news/.
[84] Bernanrd, Lunn, „Social Network Types, Motivations, and the Future“, 2017, žiūrėta 2021 m. vasario 7 d., https://readwrite.com/2007/09/12/social_network_types_motivations/.
[85] Dave Emmet, „Taxonomy of Social Networks“, 2019, žiūrėta 2021 m. vasario 7 d., https://davemmett.wordpress.com/2009/06/15/taxonomy-of-social-networks/.
[86] Michael Beye, Arjan Jeckmans, Zekeriya Erkin, Pieter Hartel, Reginald Lagendijk Qiang Tang, „Literature Overview - Privacy in Online Social Networks“, žiūrėta 2021 m. vasario 1 d., https://research.utwente.nl/en/publications/literature-overview-privacy-in-online-social-networks.

Socialinių tinklų valdytojai remdamiesi vartotojo elgsena, jo pasirinkimais, teikia jam rekomendacijas;

- verslo socialiniai tinklai. Šie socialiniai tinklai skirti profesionaliai naudingų verslo kontaktų užmezgimui. Profilių paieškai ne visada reikia registruotis šiame tinkle (pvz., „Linkedin“). Profiliai atskleidžia vartotojo galimybes ir darbo lauką, taip pat priemones susisiekti su tuo vartotoju;
- socialinių santykių (šeimos, bendraklasių ir kt.) palaikymo tinklai. Šie socialiniai tinklai nėra skirti susirasti naujų draugų, bet užmegzti ir palaikyti ryšius su esamais ar pažįstamais;
- bendravimo socialiniai tinklai. Čia vartotojai gali užmegzti ryšį su esamais draugais ir susirasti naujų. Socialinio tinklo teikėjo pajamos dažnai gaunamos iš skelbimų ir informacijos apie socialinį tinklą pardavimo. Norint pritraukti ir išlaikyti vartotojus, siūloma daugybė papildomų funkcijų. Taip pat vartotojui socialinio tinklo vertę kuria didelis draugų skaičius.

- turinio socialiniai tinklai. Turinio socialiniuose tinkluose daugiau dėmesio skiriama vartotojų teikiamam ar susietam turiniui. Skiriami dalijimosi turiniu, rekomendacijomis, patarimais, pomėgiais, naujienomis ir pramogų socialiniai tinklai:
  - turinio dalijimasis. Vartotojų sukurto turinio dalijimasis pasirinktoje grupėje, pvz., tarp draugų, šeimos narių, arba kur kas platesnėje auditorijoje. Įkeliant turinį vartotojų dažniausiai reikalaujama užsiregistruoti ir prisijungti;
  - turinio rekomendacijos. Šio tipo socialiniuose tinkluose vartotojai nekelia turinio, tačiau daugiau dėmesio skiria esamo (paprastai profesionalaus) turinio rekomendavimui;
  - pramogų socialiniai tinklai. Šie socialiniai tinklai yra susiję su žaidimų bendruomenėmis. Profilis tiesiogiai susijęs su žaidimų avataru (pseudoportretu), o ryšiai palaikomi išskirtinai tik su žaidimo nariais;
  - dalijimasis patarimais. Kai kuriuose socialiniuose tinkluose dėmesys skiriamas asmenims, norintiems dalytis savo patirtimi tam tikroje srityje, ieškant ar teikiant pagalbą ir patarimą;
  - dalijimasis pomėgiais. Daugelis socialinių tinklų orientuojasi į auditorijas, kurios turi panašių pomėgių ir interesų. Šiuose tinkluose dalijamasi rekomendacijomis ir patarimais, tačiau pagrindinis skirtumas tas, kad auditorija yra homogeniškesnė;

- dalijimasis naujienomis. Tinklaraščio pobūdžio socialiniai tinklai arba tie, kuriuose daugiausia dėmesio skiriama pasaulio naujienoms ar gandams.

Anot Nahier Aldhafferi ir kt.[87], asmens duomenys tai: biografinė informacija, dabartinė gyvenimo situacija, įskaitant gimimo datą, socialinio draudimo numerį, telefono numerį, el. pašto adresą; išvaizda, įskaitant akių spalvą, svorį, elgesys, charakterio bruožai; duomenys apie darbo vietą, išsilavinimą, gaunamą darbo užmokestį, mokamus mokesčius; duomenys apie religines, politines pažiūras, judėjimą po kitas šalis; sveikatos duomenys, įskaitant ligos istoriją, genetinius duomenis ir informaciją apie nedarbingumo laikotarpį (-ius); nuotraukos ir vaizdo įrašai; įrašai socialiniuose tinkluose.

Dahan Boyd ir Nicole Ellison[88] teigimu asmens duomenys socialiniuose tinkluose apima asmens profilį ir jo socialinius ryšius. Profilis yra susietas su pačiu vartotoju, tai jo socialinis „veidas“. Paprastai tai yra savęs pristatymas arba „alter–ego“ (pseudonimas). Socialinis ryšys – tai ryšys tarp dviejų vartotojų ir gali būti kelių tipų (draugas, bendradarbis, sekėjas ir kt.). Šias jungtis galima grafiškai atvaizduoti.

Atsižvelgiant į paslaugų tipus, kuriuos siūlo socialiniai tinklai, dažnai išskiriamos ir kitos vartotojų asmens duomenų formos[89]:

- susirašinėjimai. Tai duomenys, kuriais pasikeitė vienas vartotojas su kitu, vartotojų grupe. Vartotojų žodinė sąveika – svarbus informacijos šaltinis, daug svarbesnis nei socialinių ryšių grafikai;
- įvairialypė informacija. Informacija, kuria galima dalintis ne tik su kitais vartotojais, tačiau ir ta, kurią galima įkelti į privačią ar viešą erdvę (pvz., nuotraukų albumą, tinklaraštį, „Facebook“ sieną);
- žymos. Žymą galima apibrėžti kaip raktinį žodį, kurį vartotojas (įkėlėjas ar kiti vartotojai) prideda prie turinio. „Facebook“ socialiniame tinkle žymėjimas reiškia konkretų atvejį, kai vartotojas atpažįsta nuotraukoje pavaizduotus žmones ir pažymi nuotraukoje jų vardus, taip aiškiai susiedamas šiuos žmones su nuotrauka;
- nuostatos. Daugelis socialinių tinklų siūlo vartotojams teikia tam tikras rekomendacijas. Neretai vartotojai patys pasirenka nuostatas, kurios yra viešai matomos, o kurios – ne. Kartais rekomendacijos netiesiogiai susiformuoja dėl vartotojo elgesio socialiniame tinkle, internete;

[87] Aldhafferi Nahier, Watson Charles, Sajjev Adam, „Personal information privacy settings of online social networks and their suitability for mobile internet device“. *International Journal of Security, Privacy and Trust Management, 2* (2013): 3.
[88] Dahan Boyd, Nicole Ellison, „Social network sites: definition, history, and scholarship“. Journal of computer-mediated communication, 13 (2007), žiūrėta 2021 m. vasario 1 d., https://academic.oup.com/jcmc/article/13/1/210/4583062.
[89] Ten pat.

- grupės. Socialinio tinklo bendruomenės nariai susibūrę į grupę. Paprastai grupės taip pat naudojasi informacijos ištekliais: dalijasi nuomone, diskutuoja, kelia vaizdo informaciją ir kt.;
- informacija apie vartotojų elgseną. Elgsena socialiniame tinkle apima vartotojo naršymo istoriją ir veiksmus, kuriuos jis atlieka naršydamas tinkle. Šio tipo duomenys yra ypač vertingi. Iš jų galima spręsti apie asmenų pomėgius, socialinius ryšius, vietą ir kt.;
- prisijungimo duomenys. Siekiant naudotis socialinių tinklų teikiamomis paslaugomis, prašoma naudoti prisijungimo duomenis.

Ne visi socialiniai tinklai valdo aukščiau pateiktus vartotojų asmens duomenis. Dalis šios informacijos yra prieinama tik socialinių tinklų valdytojams, dalis prieinama ir socialinių tinklų vartotojams.

Kaip teigia Amy Loftsgordon[90], asmens teisė į privatumą socialiniuose tinkluose užtikrinama susitarus dėl tam tikrų santykių lygmens palaikymo tarp paslaugų (socialinio tinklo) teikėjams ir jų vartotojų. Taip vartotojai savo noru, laisva valia, dalį savo teisės į privatumą patiki paslaugų teikėjams, manais į galimybę būti socialinių tinklų bendruomenės dalimi, gauti geresnes nei kiti vartotojai paslaugas ir naudojimosi tinklais sąlygas, priėjimą prie kitos informacijos ir pan.

Inga Malinauskaitė[91] skiria privatumo elementus, kurie būdingi socialinių tinklų bendruomenės narių santykiams, kurie susiformuoja veikiant tinkluose: informacijos platinimas ir pasiekiamumas, asmeninės informacijos kontrolė, privatumas. Tikslinga detaliau nagrinėti kiekvieną iš jų:

- informacijos sklaida ir pasiekiamumas. Virtualaus socialinio tinklo esmė – informacijos platinimas bei pasiekiamumas. Atsižvelgiant į vartotojų lūkesčius dėl privatumo apsaugos virtualiuose socialiniuose tinkluose, tai daugelis jų nurodo asmeninės informacijos kontrolę platinant bei pasiekiant jiems reikalingą informaciją virtualiame socialiniame tinkle;
- asmeninės informacijos kontrolė. Virtualūs socialiniai tinklai pateikia privatumo nustatymus asmeninės informacijos kontrolės funkcijai įvykdyti. Vis dėlto privatumo nustatymų mechanizmai yra gana painūs ir sudėtingi, todėl daugelio asmenų informacijos kontrolė yra priklausoma taip pat ir nuo virtualių socialinių tinklų privatumo politikų;
- privatumas. Virtualiuose socialiniuose tinkluose privatumas yra suprantamas kaip vertybė palaikant ir vystant įvairius tarpasmeninius santykius. Socialinėse platformose be senųjų

[90] Amy Loftsgordon, „Social Media and Your Privacy Rights“, 2021, žiūrėta 2021 m. vasario 1 d., https://www.nolo.com/legal-encyclopedia/social-media-and-your-privacy-rights.html.
[91] Inga Malinauskaitė, „Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė“, *Social Transformations in Contemporary Society* 3, (2015): 122.

bendravimo formų (susirašinėjimas, pokalbiai) galioja ir kitokios bendravimo formos, pavyzdžiui mygtuko „patinka“ paspaudimas, komentarų po nuotraukomis rašymas bei vaizdinių įrašų žiūrėjimas. Virtualiuose socialiniuose tinkluose bendravimas vyksta žaibišku greičiu. Kiekvieną sekundę tinklą papildo daugybė naujų įrašų, po kuriais kiekvieną kartą gali būti identifikuojami konkrečių vartotojų veiksmai, kuriais siekiama užmegzti ar palaikyti tarpasmeninius santykius.

Apibendrinant galima teigti, kad vartotojai socialiniais tinklais naudojasi dėl įvairių priežasčių. Bet kokiu atveju, siekdami naudotis socialiniais tinklais, jie teikia tam tikrą informaciją. Vartotojų teikiamų duomenų tipas ir privatumas priklauso nuo socialinio tinklo ir jo teikiamų galimybių. Privatumo vertybiniai komponentai virtualiuose socialiniuose tinkluose pakito, kai privatumas nėra slapstymasis, tai yra noras kontroliuoti savo asmeninę informaciją. Šių dienų privatumas remiasi asmeninės informacijos naudojimo vengimo principais. Privatumo virtualiuose socialiniuose tinkluose pagrindiniai vertybiniai kriterijai yra: informacijos sklaida ir pasiekiamumas, asmeninės informacijos kontrolė, ribotos informacijos apie asmenį prieiga.

3.2. Prieigos prie vartotojų asmens duomenų socialiniuose tinkluose būdai

Socialiniai tinklai suteikia vartotojams galimybę sukurti išsamią paskyrą ir užmegzti ryšį su kitais vartotojais, ypatingą dėmesį skiriant socialiniams ryšiams. Kaip teigia Danah M. Boyd ir Nicole B Ellison[92], šie tinklai gali suteikti galimybę keistis informacija (lytis, amžius, pomėgiai, išsilavinimo istorija ir užimtumas, taip pat muzikos, nuotraukų, vaizdo įrašų rinkmenos ir nuorodos) su kitais registruotais vartotojais. Šie tinklai dažnai gali keistis registruotų vartotojų duomenimis naudodamiesi nuorodomis į asmenis ir programas.

Yra keli būdai, kaip trečiosios šalys gali pasiekti privačią asmenų – socialinių tinklų vartotojų informaciją, tikslinga pateikti svarbiausius.

Būsenos atnaujinamas socialiniame tinkle. Anot Sushama ir Sunil Kamar[93], socialiniai tinklai leidžia vartotojams pakeisti būseną kada jie tik to nori. Šie tinklai yra sukurti taip, kad lengvai ir laisvai galima keisti informaciją, o privatumo nustatymai yra tam, kad būtų išvengta grėsmių, susijusių su pasikeitusia būsena.

[92] Danah M. Boyd, Nicole B. Ellison, „Social network sites: definition, history, and scholarship“, *IEEE English Management Review* 38 (3) (2010).
[93]Carl Sushama, Sunil Kumar, Paul Neelima, „ Privacy and security issues in the future: A social media. Materials Today“, *Proceedings 1(7)* (2021).

Privačių asmens duomenų dalijimasis su trečiosiomis šalimis. Įrodyta, kad „Facebook“ programos: „Farmville“, „Causes“ ir „Quiz Planet“ dalijosi vartotojų privačiais duomenimis su reklamos bendrovėmis. Jei vartotojas spustelėdavo konkretų skelbimą puslapyje, „Facebook“ išsiųsdavo reklamuotojams šio puslapio vartotojo profilio adresą. Tokiu atveju lengva nustatyti tikruosius vartotojų vardus ir kitą informaciją[94]. Dar vienas plačiai žinomas atvejis, anot Joanne Hinds ir kt.[95], kai „Cambridge Analytica“ rinko vartotojų duomenis, jiems sutikus užpildyti psichologinio vertinimo klausimyną. „Cambridge Analytica“ galėjo ne tik susipažinti su apklausoje dalyvavusio asmens duomenimis, bet ir gavo priėjimo prie draugų rato duomenų.

Aplikacijų programavimo sąsaja (angl. *API*). Ši sąsaja leidžia programinei įrangai „kalbėti“ su kita programine įranga. Be to, aplikacijų programavimo sąsaja gali rinkti ir apdoroti informaciją, kuri nėra viešai prieinama. Tai itin aktualu tyrėjams, nes gali pasiekti didesnį tiriamųjų skaičių. Sąsajos naudojamos renkant duomenis, ir nors duomenys gali būti privatūs, programai sunku atpažinti, kada jie tampa asmens privatumo saugos pažeidimu. Dėl sąsajos taikymo kilo skandalas su „Cambridge Analytica“. „Facebook“ leido trečiosios šalies bendrovei sukurti programą tam tikslui, kad būtų renkami duomenys. Kūrėjas pasinaudojo spraga ir rinko informaciją ne tik apie vartotojus, kurie naudojosi programa, bet ir apie jų draugų ratus, jiems nežinant[96].

Paieškos sistemos. Joanne Hinds ir kt.[97] teigimu, paieškos sistemos yra paprastas būdas rasti kitą vartotoją, grupę ar prekių/paslaugų pardavėją ir kt. Į paieškos lauką įvedus raktinius žodžius pateikiami paieškos rezultatai. Būtina įsitikinti, kad įvesti raktiniai žodžiai yra tikslūs ir teisingi. Yra daugybė profilių, kurie gali nukreipti vartotoją į netikras svetaines, su tikslu gauti asmeninės informacijos, arba šios svetainės būna apkrėstos virusais.

Vietos duomenys. Daugumoje socialinių tinklų geografinę vietą gali nurodyti patys vartotojai (žymėdami savo buvimo vietą). Sushama ir Sunil Kamar[98] teigimu, taikomas metodas turi mažiau reikšmės nei rezultatas, ar sukurtas turinys, kuris yra susietas su geografine vieta. Be to, programos prideda kitos papildomos informacijos, tokios kaip, kokią operacinę sistemą naudoja vartotojas, kokį mobilų telefoną turį, kokiu laiku buvo įkeltas turinys ir pan. Rezultatas yra tas, kad vartotojai, skelbdami, fotografuodami, sukuria ir dalijasi savo asmenine informacija.

---

[94] Ari Ezra Waldman, „*Privacy, Sharing, and Trust: The Facebook Study*“, Žiūrėta 2021 m. balandžio 1 d., https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=4679&context=caselrev.

[95] Joanne Hinds, Emma J. Williams, Adam N. Joinson, „“It wouldn't happen to me”: Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies 143* (2020).

[96] Ten pat.

[97] Ten pat.

[98] Carl Sushama, Sunil Kumar, Paul Neelima, „ Privacy and security issues in the future: A social media. Materials Today“, *Proceedings 1(7)* (2021).

Apibendrinant galima teigti, kad vartotojų turinys socialiniuose tinkluose apima vartotojų patirtį, nuomones ir žinias. Be to, turinys taip pat apima asmeninius duomenis, pvz., vardą, lytį, buvimo vietą ir privačias nuotraukas (vaizdo įrašus). Socialinių tinklų vartotojai neretai susiduria su socialinio identiteto valdymo iššūkiais, tuo pačiu keldami grėsmę savo asmeniniam privatumui. Asmenys jaučiasi sekami, o tinklų veiklos monetizavimas, skatina rinkti informacija apie tinklų vartotojus, siekiant kontroliuoti rinką. Socialinių tinklų naudojami įrankiai (būsenos atnaujinamas socialiniame tinkle, privačių asmens duomenų dalijimasis su trečiosiomis šalimis, aplikacijų programavimo sąsaja, paieškos sistemos, vietos duomenys) pakeitė vartotojų sąveiką asmeniniame ir profesiniame gyvenime, bei tačiau tuo pačiu kelia ir didelę riziką, susijusią su asmens privatumu ir saugumu. Vartotojai, kurie reguliariai naudojasi socialiniais tinklais, yra įvairių sukčių, nusikaltėlių ar vartotojų elgsenos tyrimo grupių taikinys.

3.3. Asmens privatumo saugos socialiniuose tinkluose pažeidimo būdai

Socialiniai tinklai gali kelti įvairių grėsmių jų vartotojams, dėl galimybės pasiekti daug asmeninės informacijos, kurią atskleidžia patys vartotojai. Kaip teigia Ahmad Ali ir kt.[99], dažniausiai kėsinamasi į privačią asmenų informaciją, skaitmeninę tapatybę, finansinį turtą, intelektinę nuosavybę. Toliau nagrinėjami įprasti asmens privatumo saugos pažeidimo būdai socialiniuose tinkluose.

Socialinė inžinerija ir atvirkštinės socialinės inžinerijos atakos (angl. *social engineering and reverse social engineering attacks*). Edwin Donald Frauenstein ir Stephen Flowerday[100] teigimu, socialinės inžinerijos atakos vyksta, kadangi socialinių tinklų vartotojai nežino tikrosios privačios informacijos vertės ir svarbos, jie neskiria reikiamą dėmesį, siekiant apsisaugoti nuo kenkėjiškų programų, asmenų išpuolių. Tokioje situacijoje trečiosios šalys gali apgauti vartotojus atskleisti konfidencialią informaciją, pasitelkiant skirtingus mechanizmus. Pavyzdžiui, sukčiavimas (žvejyba arba fišingas) (angl. *fishing*) yra sukčiavimo forma, siekiant iš vartotojų išvilioti konfidencialius duomenis, naudojant nuorodas į kitas interneto svetaines. Taip pat skiriamos šios socialinės inžinerijos atakos formos: masalas (angl. *baiting*) ir pasitikėjimas (angl. *tailgaiting*). Kaip teigia Ajith Sundaram[101], atvirkštinė socialinės inžinerijos ataka yra dar viena grėsmė socialiniams tinklams ir jų vartotojams. Ataka vyksta kenkėjui apgavus vartotoją susisiekti su juo, naudodamas įvairaus pobūdžio metodus. Kadangi vartotojas užmezga ryšį, kenkėjas pradeda savo veiksmus (pvz., sukčiavimas, šlamšto siuntimas ir kt.).

[99] Ali Ahmad, Ahmad Kamran Malik, Mansoor Ahmed, Basit Raza, „Privacy Concerns in Online Social Networks: A Users' Perspective", *International Journal of Advanced Computer Science and Applications 10(7)* 2019.
[100] Frauenstein Edwin Donald, Stephen Flowerday. „Susceptibility to phishing on social network sites: A personality information processing model", *Computers & Security 94* (2020).
[101] Ajith Sundaram, „Understanding and Protecting Yourself against Threats in the Internet", *Asian Social Science 13 (12)*.

Francesco Colace ir kt.[102] pateikia socialinės inžinerijos atakos pavyzdį, kai 2012 m. kovo mėn. įvyko socialinės inžinerijos ataka, kurio metu buvo sukurta netikra admirolo James Stavridis, NATO vyriausiojo sąjungininkų Europoje vado (SACEUR), paskyra, siekiant apgauti jo draugus ir kolegas, su tikslu su juo susisiekti ir atskleisti konfidencialią informaciją, taikant socialinės inžinerijos metodus. Pranešus apie netikrą profilį „Facebook“, jis buvo deaktyvuotas ir pradėtas tyrimas, siekiant nustatyti nusikaltimo organizatorius ir vykdytojus.

Tapatybės vagystė (angl. *identity theft*). Tapatybės vagystė yra vienas iš asmens privatumo saugos socialiniame tinkle pažeidimo būdų. Kaip teigia Ahmad A. Al–Daraiseh ir kt.[103], vagis siekia surinkti socialinių tinklų vartotojų asmeninę informaciją, siekiant naudos ir/ar norint pakenkti. Tapatybės vagystės atakoms naudojami skirtingi metodai: sukčiavimas, nepažįstamų žmonių užklausos draugauti priėmimas, pasidalijimas paskyros informacija su kitais, nuorodų spustelėjimas, nukreipiančių vartotoją į kitas svetaines, nemokamų programų atsisiuntimas, žemo lygio privatumo nustatymai ir kt.

Šlamšto atakos. Anot Sepideh Deliri and Massimiliano Albanese[104], pagrindinis šlamšto siuntėjų tikslas yra išsiųsti kuo daugiau pranešimų, kuriuose reklamuojami ir parduodami jų produktai, su siekiu gauti kuo privačių duomenų apie vartotojus (pvz., vartotojo vardas ir slaptažodis), apsimetant patikimu prekių ir paslaugų tiekėju (pvz., bankų darbuotoju). Šią informaciją galima gauti naudojant suklastotus socialinių tinklų profilius, kuriuos sukūrė sukčiai. Taikydami šį metodą, sukčiai siunčia atsitiktines užklausas draugautis socialinio tinklo tikslinės bendruomenės nariams, laukdami, kol jie juos priims.

Kenkėjiškos programos. Kaip teigia Julian Jang–Jaccard ir Surya Nepal[105], kenkėjiškos programos (angl. *phishing*) skirtos pakenkti kompiuterinėms sistemoms arba kontroliuoti jų veikimą siekiant įgyti asmenų privačius duomenis. Kenkėjiškos programos gali lengvai išplisti socialiniame tinkle dėl to, kad šis tinklas jungia didžiulį vartotojų skaičių, turi plačią komunikacijos infrastruktūrą. Tai sukčiams palanki platforma, leidžiančią lengvai plisti tarp vartotojų ir pasinaudoti jų asmeniniais duomenimis. Pavyzdžiui, „Koobface“ buvo pirmoji kenkėjiška programa, išplitusi daugelyje socialinių tinklų, įskaitant „Facebook“ ir „Twitter“. 2008 m. „Koobface“ iš pradžių pasklido „Facebook“, perduodamas užkrėsto vartotojo žinutes „Facebook“ draugams. Pranešimas galėjo būti išsiųstas iš netikros paskyros, kurią sukūrė pati „Koobface“ ir, kuri automatiškai užmezgė draugystę su socialinių

[102] Francesco Colace, Massimo De Santo, Vincenzo Moscato Antonio Picariello, Fabio Schreiber Letizia, „*Data Management in Pervasive Systems*“, Žiūrėta 2021 m. balandžio 1 d., https://link.springer.com/book/10.1007%2F978-3-319-20062-0.
[103] Ali Ahmad, Ahmad Kamran Malik Mansoor, Ahmed Basit Raza, „Privacy Concerns in Online Social Networks: A Users‘ Perspective“, *International Journal of Advanced Computer Science and Applications 10(7)* 2019.
[104] Sepideh Deliri, Massimiliano Albanese, „Security and Privacy Issues in Social Networks“. Data Management in Pervasive Systems. (Cham: Springer, 2015).
[105] Julian Jang-Jaccard, Surya Nepal, „A survey of emerging threats in cybersecurity“, *Journal of Computer and System Sciences 80(5) 2014*: 973.

tinklų vartotojais. Į pranešimą buvo įtrauktas universalus adresas (angl. *URL*), kuris nukreipė susidomėjusius vartotojus į suklastotą „Facebook“ puslapį ir apgaule įdiegė „Koobface“ kenkėjišką programą. Pagrindinis „Koobface“ tikslas buvo pavogti asmeninę vartotojų informaciją, įskaitant jų prisijungimo informaciją, ir pradėti piktavališką veiklą, pavyzdžiui, siųsti šlamšto žinutes. Dar vienas iš pavyzdžių, kai 2019 m. rugpjūčio mėn. kenkėjiška programa buvo nukreipta į „Instagram“ vartotojus, apgavus, kad yra dviejų veiksnių autentifikavimo sistema, paskatinanti vartotojus prisijungti prie klaidingo „Instagram“ puslapio.

Ataka paspaudus nuorodą (ar paspaudus „patinka“ mygtuką) (angl. *clickjacking, likejacking, and cursorjacking attacks*). Sepideh Deliri and Massimiliano Albanese[106] teigimu, tokio tipo atakose kenkėjiška trečioji šalis apgauna socialinių tinklų vartotojus, kai jie spusteli nuorodą, kuri yra visai ne tai, ko jie tikėjosi. Kitaip tariant, vartotojui rodomas tinklalapis skiriasi nuo puslapio, į kurį norėjo patekti nuorodą paspaudęs vartotojas. Kaip pavyzdį galima pateikti atvejį „Facebook“, įvykusį 2009 m. gruodžio mėn. „Facebook“ vartotojai spustelėję nuorodą, paskelbtą draugo tinklalapyje, pateko į „YouTube“ puslapį, kuriame buvo reklamuojamos prekės.

Skriptai (angl. *cross-cite scripting*) yra tam tikros rūšies ataka prieš socialinius tinklus ir jų vartotojus, kai įterpiamas kenkėjiškas kodas į tinklalapius ir paspaudus nuorodą, vartotojai šie kodą paleidžią, siekiant pavogti jų asmeninius duomenis[107].

Patyčios socialiniuose tinkluose (angl. *cyberbulling*) – tam tikros rūšies ataka, kurios metu tiksliniams vartotojams siunčiama kenksminga ar įžeidžianti medžiaga, įskaitant tekstą ir vaizdus. Kai vartotoją (-us) įžeidžianti informacija pasklinda didelėje socialinio tinklo vartotojų grupėje, sudėtinga ją pašalinti iš tinklo. Patyčios socialiniuose tinkluose dažnai vyksta anonimiškai; todėl atsekti jų šaltinį ne visada yra lengva užduotis. Neigiamos patyčių atakų pasekmės gali būti pražūtingos vartotojams. Jie gali jaustis susierzinę, nesaugūs, pikti ar pažeminti[108].

Sukčiavimas (angl. *internet fraud*). Anot Julian Jang–Jaccard ir Surya Nepal[109], remiantis vartotojų skaičiaus dinamika, investuotojai gali naudoti socialinį tinklą kaip informacijos šaltinį priimant finansinius sprendimus, todėl vartotojų skaičiaus pokyčiai gali būti panaudoti įvairių tipų sukčiavimui. Pavyzdžiui, siekdami finansinės naudos gali būti dirbtinai didinamas vartotojų skaičius. Taip pat

[106] Sepideh Deliri, Massimiliano, Albanese, „Security and Privacy Issues in Social Networks“. Data Management in Pervasive Systems. (Cham: Springer, 2015).
[107] Ten pat.
[108] Ten pat.
[109] Julian Jang-Jaccard, Surya Nepal, „A survey of emerging threats in cybersecurity“, *Journal of Computer and System Sciences 80(5) 2014*: 973.

sukčiavimo atvejai galimi, kai siekiant padidinti vartotojų skaičių, apgaule pasisavinamos asmens tapatybės, pasinaudojama jų kreditinėmis/debitinėmis kortelėmis.

Duomenų gavyba ir išpuoliai (angl. *data mining and inference attacks*). Visi besinaudojantys socialiniais tinklais palieka „pėdsakus“ jame. Kiekvieną kartą, kai kas nors sukuria naują paskyrą, jis pateikia savo asmeninę informaciją: vardą, gimimo datą, gyvenamąją (geografinę buvimo) vietą ir asmeninius interesus. Be to, socialinių tinklų tiekėjai renka duomenis apie vartotojų elgseną: kada, kur ir kaip vartotojai sąveikauja naudodamiesi platforma. Visi šie duomenys yra saugomi ir naudojami, siekiant geriau nukreipti reklamą. Kartais socialinių tinklų teikėjai dalijasi vartotojų duomenimis su trečiosiomis šalimis, dažnai be vartotojų žinios ar sutikimo[110]. Anot Sepideh Deliri and Massimiliano Albanese[111], duomenų gavyba yra galinga priemonė tyrėjų siekiant gauti naudingos informacijos iš didelių duomenų kiekių. Nors informacija, surinkta iš socialinių tinklų vartotojų, naudojant duomenų gavybos metodus, gali būti naudingas šaltinis gerinant socialinių tinklų veiklą ir teikiamų paslaugų kokybę, tačiau šią informaciją galima panaudoti siekiant išgauti žinias, kurios gali pakenkti vartotojų privatumui. Trečiosios šalys gali pasinaudoti socialinių tinklų vartotojų atskleista informacija, siekdami surinkti papildomų neskelbtinų duomenų apie juos. Naudodamiesi algoritmais, trečiosios šalys surinkti asmenų privačius duomenis (pvz., vartotojų draugų ratas, nuostatos ir pomėgiai ar politinės pažiūros).

Apibendrinant galima teigti, kad pagrindiniai asmens privatumo saugos socialiniuose tinkluose pažeidimo būdai yra: socialinės inžinerijos ir atvirkštinės socialinės inžinerijos atakos, tapatybės vagystės, šlamšto atakos, kenkėjiškų programų diegimas, ataka paspaudus nuorodą, skriptai, patyčios socialiniuose tinkluose, sukčiavimas, duomenų gavyba ir išpuoliai). Užtikrinant asmens privatumo saugą socialiniuose tinkluose susiduriama su trimis pagrindinėmis problemomis: privatumas, vientisumas ir prieinamumas. Socialinių tinklų inžinieriai turėtų siekti ne tik apsaugoti vartotojų asmeninę informaciją ir turinį, kuriuo jie dalijasi savo sienoje, profilyje, bet ir siekiama, kad socialinių tinklų narių naudojami komunikacijos kanalai būtų apsaugoti nuo vidinių ar išorinių išpuolių, kad trečiosios šalies vartotojai negalėtų patekti į juos. Taip pat siekiama užkirsti kelią trečiosioms šalims sužinoti, kurie vartotojai tarpusavyje bendrauja. Galiausiai, turi būti įdiegti prieigos kontrolės mechanizmai, užtikrinant, kad turinys būtų prieinamas vartotojams, kuriems buvo suteiktas leidimas pasiekti tokį turinį.

[110] Tulane University, „Key Social Media Privacy Issues for 2020“, 2021, žiūrėta 2021 m. balandžio 19 d., https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020.
[111] Sepideh Deliri, Massimiliano Albanese, „*Security and Privacy Issues in Social Networks*“. Data Management in Pervasive Systems. (Cham: Springer, 2015).

4. ASMENS PRIVATUMO SAUGOS SOCIALINIUOSE TINKLUOSE ĮGYVENDINIMO PROBLEMOS PRAKTIKOJE

4.1. Socialinio tinklo „Facebook" ir „Cambridge Analytica" atvejo poveikis asmens privatumo saugumui socialiniuose tinkluose įgyvendinimui

Socialinis tinklas „Facebook" ne kartą susidūrė su asmens privatumo apsaugos pažeidimais. Anot Amelia D. Grubbs[112], dar 2007 m. „Facebook" buvo pateiktas ieškinys dėl slapukų naudojimo. Dan Petterson teigimu, socialinis tinklas slapukų pagalba sekė vartotojų veiklą, ir tai laikoma kaip vienas iš ankstyviausių kompanijos bandymų monetizuoti vartotojų duomenis[113]. Maždaug po ketverių metų Federalinės prekybos komisija[114] tyrė „Facebook" veiklą dėl to, kaip įmonė dalijosi privačių vartotojų duomenimis su trečiųjų šalių įmonėmis. Šis tyrimas buvo pradėtas dėl to, kad „Facebook" 2009 m. pakeitė paslaugų teikimo vartotojams sąlygas ir leido naudoti bet kokį turinį, kurį paskelbė, įkėlė vartotojas, neatsižvelgiant į tai, koks „Facebook" duomenų rinkimo tikslas ir, kokiu tikslu valdomi duomenys, jeigu vartotojas yra išaktyvavęs „Facebook" paskyrą. 2013 m. „Facebook" pranešė apie klaidą jų programinėje įrangoje[115], dėl kurios buvo atskleisti šešių milijonų paskyrų asmeniniai duomenys. Šią klaidą rado vartotojai, bandę atsisiųsti savo „Facebook" veiklos istoriją, tuo pačiu gavę prieigą prie savo ir draugų adresų knygų duomenų. Akivaizdu, kad „Facebook" nuo pat savo veiklos pradžios iki 2013 m. ne kartą netinkamai naudojo ir tvarkė savo vartotojų duomenis. Iki 2013 m. „Facebook" aplaidumas sukėlė santykinai nedidelio poveikio pasekmes, patyrė nedidelius nuostolius, gavo švelnias Federalinės prekybos komisijos ir kitų vyriausybės institucijų nuobaudas. Tačiau, anot Ahmad Ali ir kt.[116], tai, kad valdomi duomenys tapo labai pažeidžiami, tapo didele grėsme socialinio tinklo vartotojų privatumo saugumui. Šios spragos galiausiai ir lėmė duomenų nutekinimo „Cambridge Analytica" skandalą. 2013 m. Kembridžo universiteto mokslininkai paskelbė straipsnį[117], kuriame

---

[112] Amelia D. Gubbs, „*Privacy Law and the Internet using Facebook.com as a Case Study Study*" (Chancellor's Honors Program Projects: 2011), žiūrėta 2021 m. balandžio 19 d., https://trace.tennessee.edu/cgi/viewcontent.cgi?article=2397&context=utk_chanhonoproj.

[113] Dan Petterson, „*Facebook data privacy scandal: A cheat sheet*", Žiūrėta 2021 m. balandžio 1 d., https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.

[114] Federal Trade Commission, „*Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*", 2011, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

[115] Todd DeCapua, „*How a software bug slammed Facebook users*", žiūrėta 2021 m. balandžio 19 d., https://techbeacon.com/app-dev-testing/how-software-bug-slammed-facebook-users.

[116] Ali Ahmad, Ahmad, Kamran Malik, Mansoor, Ahmed, Basit, Raza, „Privacy Concerns in Online Social Networks: A Users' Perspective", *International Journal of Advanced Computer Science and Applications 10(7)* 2019.

[117] Michael Kosinski, David Stillwell, „*Digital records could expose intimate details and personality traits of millions*", 2013, žiūrėta 2021 m. balandžio 19 d., https://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions.

išsamiai aprašyta, kaip remiantis „Facebook“ duomenis galima nustatyti žmonių savybes, pomėgius, prognozuoti elgseną. Tyrėjai perspėjo, kad tyrimo išvados gali kelti grėsmę asmens privatumui, gerovei, laisvei ar net gyvybei. Šie mokslininkų įspėjimai liko nepastebėti.

„Cambridge Analytica“ 2013 m. įkūrė buvęs „Breitbart News Network“[118] vyriausiasis redaktorius Steve Bannon ir Robert Mercer („Renaissance Technologies“[119] generalinis direktorius). Šios įmonės siekis buvo pasinaudoti socialinių tinklų duomenimis ir paveikti žmonių požiūrį ir elgseną politiniais tikslais. Pasitelkdama taikomąją programą ir bendradarbiaudama su „Facebook“, „Cambridge Analytica“ surinko duomenis iš vartotojų[120]. Kimberly A. Houser ir W. Gregory Voss[121] teigimu, apie 250 000 asmenų sutiko su „Cambridge Analytica“ sąlygomis įsigyti ir analizuoti jų duomenis, mainais į galimybę pasinaudoti jų siūloma taikomąja programa. Tačiau įmonė pasitelkdama programą pasinaudojo vartotojais, siekiant surinkti duomenis apie juos ir jų draugų ratą. „Cambridge Analytica“ pasinaudodama įgytais duomenis sukūrė psichologinius vartotojų profilius. Warwick universiteto atliktu tyrimu[122] nustatyta, kad šie profiliai buvo naudojami Donald Trump prezidento kampanijai kuriant politinius skelbimus, siekiant paveikti neapsisprendusių rinkėjų nuomonę ir elgseną rinkimų metu.

2015 m. gruodžio mėn. „The Guardian“ paskelbė straipsnį[123], atskleidžiantį, kad „Cambridge Analytica“ naudojo „Facebook“ duomenis, kad padėtų senatoriui Ted Cruz tapti respublikonų kandidatu į prezidentus. Kogan (Kembridžo universiteto psichologas) informavo „Facebook“, kad duomenys buvo naudojami tik akademiniams tikslams, o „Facebook“ patikėjo tuo, kas sakoma nepatikrinus, ar tai tiesa[124]. Tačiau 2019 m. „The Guardian“ tyrimas[125] atskleidė, kad „Facebook“ dar 2015 m. žinojo apie

---

[118] „Breitbart News Network“ yra amerikiečių kraštutinių dešiniųjų sindikuotų naujienų, nuomonių ir komentarų svetainė, kurią 2007 m. Viduryje įkūrė amerikiečių konservatorių komentatorius Andrew Breitbartas.

[119] Amerikos rizikos draudimo fondas, kurio specializacija yra sisteminė prekyba, naudojant kiekybinius modelius, gautus iš matematinės ir statistinės analizės.

[120] Iva Nenadic, „Unpacking the „European approach" to tackling challenges of disinformation andpolitical manipulation“, *Internet policy review, 8(4)* 2019.

[121] Kimberly A. Houser, W. Gregory Voss, „GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?“, *SSRN Electronic Journal*, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.researchgate.net/publication/326755233_GDPR_The_End_of_Google_and_Facebook_or_a_New_Paradigm_in_Data_Privacy.

[122] University of Warwick. „Targeted Facebook ads shown to be highly effective in the 2016 US Presidential election." *ScienceDaily*, , žiūrėta 2021 m. balandžio 19 d., www.sciencedaily.com/releases/2018/10/181025103303.htm.

[123] Harry Davis, „*Ted Cruz using firm that harvested data on millions of unwitting Facebook users*“, 2015, žiūrėta 2021 m. balandžio 19 d., https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.

[124] Carole Cadwalladr, „*I created Steve Bannon's psychological warfare tool': meet the data war whistleblower*“, The Cambridge Analytica Files, 2018, Žiūrėta 2021 m. balandžio 1 d., http://www.hec.unil.ch/lspinto/Papers%20&%20CV/The%20Cambridge%20Analytica%20Files.pdf.

[125] Julia Carrie Wong, „*Document reveals how Facebook downplayed early Cambridge Analytica concerns*“, 2019, Žiūrėta 2021 m. balandžio 1 d., https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document.

„Cambridge Analytica“ ketinimus rinkti duomenis, kaip ir „Cambridge Analytica“ dalyvavimą Ted Cruz kampanijoje.

Vidinė „Facebook“ darbuotojų komunikacija atskleidė[126], kad 2015 m. rugsėjo 22 d. „Facebook“ darbuotojas (darbuotojas „X“) išreiškė susirūpinimą dėl įmonių, naudojančių „Facebook“ duomenis, ir norėjo sužinoti daugiau apie „Facebook“ politiką, susijusią su trečiųjų šalių prieiga prie vartotojų duomenų. Darbuotojas „X“ įtarė, kad daugelis bendrovių atlieka panašius veiksmus, didžiausia ir agresyviausia yra„ Cambridge Analytica“ – duomenų modeliavimo įmonė, kuri giliai įsiskverbusi į rinką. Prie darbuotojo „X“ įtarimų prisijungė nedidelė kitų „Facebook“ darbuotojų grupė, ir paprašė administracijos ištirti, ką „Cambridge Analytica“ daro su jų pateiktais vartotojo duomenimis. Tačiau „Facebook“ nevykdė tyrimo motyvuodami: „...<...> trečiųjų šalių įmonės nepažeidžia nė vienos iš mūsų sąlygos <...> jei turėtume daugiau įrodymų, vertintume, tačiau šiuo keliu eisime tik tuo atveju, jei įžvelgsime grėsmes“[127].

Anot Iga Kozlowska[128], „Facebook“ sąmoningai nusprendė netirti „Cambridge Analytica“ veiklos. „Facebook“ nesiėmė veiksmų prieš „Cambridge Analytica“ iki pat 2016 m. rugpjūčio mėn., kuomet teisininkai raštu kreipėsi „Cambridge Analytica“, prašydami ištrinti visus surinktus vartotojų duomenis. Nors „Cambridge Analytica“ pranešė „Facebook“, kad surinktus duomenis ištrynė, tačiau „Facebook“ negalėjo patikrinti, ar reikalavimas įgyvendintas. Taigi Facebook“ veiksmai „Cambridge Analytica“ atžvilgiu buvo aplaidūs ir pasyvūs.

2018 m. kovo 17 d. duomenų analitikas Christopher Wylie, anksčiau dirbęs „Cambridge Analytica“, visuomenei atskleidė, kad „Cambridge Analytica“ surinko daugiau nei 87 milijonų „Facebook“ vartotojų duomenis[129]. Po šio pranešimo „Facebook“ tylėjo iki kovo 21 d., tuomet Mark Zuckerberg galiausiai paskelbė oficialų įrašą „Facebook“ apie tai, kaip „Facebook“ yra atsakinga už savo vartotojų duomenų apsaugą, kurios nepavyko užtikrinti bendradarbiaujant su „Cambridge Analytica“. To pasėkoje, „Facebook“ generalinis direktorius Mark Zuckerberg buvo iškviestas į Senato Prekybos ir Senato Teismų komitetus, pasiaiškinimui.

---

[126] Jerrold Nadler, David N., *Cicilline, „Investigation of Competition in Digital Markets*“ (United States: 2020), Žiūrėta 2021 m. balandžio 1 d., https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.

[127] Ten pat, 146 p.

[128] Iga Kozlowska, „*Facebook and Data Privacy in the Age of Cambridge Analytica*“ (Washington: University of Washington, 2018), Žiūrėta 2021 m. balandžio 19 d., https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/.

[129] *Mark Zuckerberg's Wednesday testimony to Congress on Cambridge Analytic*a, Žiūrėta 2021 m. balandžio 1 d., https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978.

Remiantis Federalinės prekybos komisija duomenimis[130], po vienerių metų tiriant „Cambridge Analytica“ veiklą, 2019 m. liepos 24 d. „Facebook“ buvo skirta 5 milijardų dolerių bauda – didžiausia bauda, kada nors paskirta už duomenų saugos pažeidimą. Taip pat Federalinės prekybos komisija įpareigojo „Facebook“ atlikti eilę reikalavimų užtikrinant vartotojų privatumo saugumą[131]. Federalinės prekybos komisija[132] įpareigojo „Facebook“ kas ketvirtį rengti ataskaitas ir suformuoti komitetą (su keletu nepriklausomų narių) atsakingą už asmens privatumo saugos kontrolę. Bendrovė taip pat buvo įpareigota sumokėti 100 milijonų dolerių baudą JAV saugumo ir mainų komisijai, nes „Facebook“ neatskleidė savo investuotojams informacijos, kurią turėjo apie „Cambridge Analytica“ veiksmus.

Po įvykusio Energijos ir Komercijos komiteto posėdžio[133], „Facebook“ ėmėsi veiksmų, siekiant sumažinti keitimosi vartotojų duomenimis su trečiosiomis šalimis tikimybę, siekiant išvengti kito duomenų privatumo pažeidimo skandalo. Senato ir įstatymų leidėjų paklaustas apie didesnio privačių vartotojų duomenų reguliavimo idėją, Mark Zuckerbergas sutiko teigdamas: „manau, kad tai aktuali problema, nes internetas tampa vis svarbesnis žmonių gyvenime, todėl būtinas tinkamas asmens privatumo saugumo reguliavimas“[134]. „Facebook“ generalinis direktorius taip pat pasiūlė JAV įgyvendinti griežtesnę interneto reguliavimo politiką, panašią į Europos bendrąjį duomenų apsaugos reglamentą, kuriame numatytos griežtos baudos įmonėms, pažeidžiančioms duomenų privatumo politiką[135]. 2019 m. kovo 6 d. Mark Zuckerberg savo „Facebook“ paskyroje paskelbė įrašą pavadinimu „Socialinės žiniasklaidos vizija į privatumą“[136], kurioje jis pabrėžia asmens privatumo saugumo svarbą ir pristato „Facebook“ viziją, sutelkiant dėmesį į asmens privatumo užtikrinimą šifruojant duomenis.

---

[130] Federal Trade Commission, „*FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*“, 2019, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[131] Mary Craft, „*Big data, little privacy: protecting consumers' data while promoting economic growth*“, Žiūrėta 2021 m. balandžio 1 d., https://www.reminger.com/media/publication/15075_BIG%20DATA%20LITTLE%20PRIVACY%20PROTECTING%20CONSUMERS%20DATA%20WHILE%20PROMOTING%20ECONOMIC%20GROWTH.pdf

[132] Federal Trade Commission, „*FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*“, 2019, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[133] Committee on Energy and Commerce, „*Hearing before the Committee on Energy nad Commerce House of Representatives. One hundred fifteen Congress. Second Session. Facebook transparency and use of consumer data*“, žiūrėta 2021 m. balandžio 19 d., https://www.govinfo.gov/content/pkg/CHRG-115hhrg30956/pdf/CHRG-115hhrg30956.pdf.

[134] *Mark Zuckerberg's Wednesday testimony to Congress on Cambridge Analytica*, Žiūrėta 2021 m. balandžio 1 d., https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testimony-to-congress-on-cambridge-analytica-509978.

[135] Noam Kolt, „Return on Data: Personalizing Consumer Guidance in Data Exchanges“, *Yale Law & Policy Review, 38 (77)* 2019.

[136] Mark Zuckerberg, „*A Privacy-Focused Vision for Social Networking*“, žiūrėta 2021 m. balandžio 19 d., https://www.facebook.com/notes/2420600258234172/.

„Facebook“ elgesio kodekso[137] 8 skyrius nustato vartotojo duomenų ir personalo duomenų apsaugą. Šiame skyriuje aptariama „Facebook“ darbuotojų, kurie turi prieigą prie vartotojų duomenų, atsakomybė, kuri įgyvendinama saugojant neskelbtinus konfidencialius vartotojo duomenis. „Facebook“ elgesio kodekse nurodoma, kad darbuotojams suteikiama prieiga prie duomenų tik tiek, kiek to reikia siekiant darbą. 8 skyriuje taip pat aptariamas „Facebook“ vartotojų duomenų jautrumas ir konfidencialumas, vartotojų duomenų apsaugos svarba. Pagrindžiant „Facebook“ neveiksnumą paminėta, kad dar 2015 m. „Facebook“ aukštesnes pareigas užimantys darbuotojai[138] nekreipė dėmesį į darbuotojų susirūpinimą dėl „Cambridge Analytica“ duomenų naudojimo. „Facebook“ darbuotojų neveiksnumas „Cambridge Analytica“ atveju akivaizdžiai rodo, kad jie pažeidė elgesio kodeksą, kadangi žinojo, kad „Cambridge Analytica“ vartotojų duomenis naudojo ne pagal numatytą paskirtį, tačiau nieko nedarė.

„Facebook“ duomenų politikos 3 skyriuje[139], „Bendrinimas su trečiosios šalies partneriais“ savo vartotojus informuoja, kad tyrėjams ir akademikams suteikia prieiga prie „Facebook“ duomenų ir jiems leidžiama atlikti tyrimus, kurie skatina aukštesnį išsimokslinimą ir naujoves, prisidedančias prie bendrovės verslo ar misijos sėkmės, bei plėtojančias atradimus ir naujoves, susijusius su bendrąja socialine gerove, technologine pažanga, viešaisiais interesais, sveikata ir gerove. „New York Times“ dienraščio žurnalistų atliktas tyrimas[140] atskleidė, kaip „Cambridge Analytica“ darbas su prezidento D. Trumpo kampanija buvo neigiamai paveikęs 2016 m. Jungtinių Valstijų visuotinius rinkimus ir nedidino visuomenės gerovės, pažangos.

Po to, kai 2018 m. Christopher Wylie pranešė apie „Cambridge Analytica“ netinkamo duomenų naudojimo mastą, „Facebook“ akcijos iš pradžių smuko 8 proc.[141] Nepaisant naujienų apie skandalą, „Facebook“ pelnas, tenkantis vienai akcijai, 2018 m. pabaigoje augo 40 proc., lyginant su praėjusių metų rezultatais[142]. „Facebook“ kontroliuoja maždaug du trečdalius arba 70 proc. suaugusiųjų, kurie naudojasi

---

[137] Facebook, „*Code of Conduct*“, Žiūrėta 2021 m. balandžio 1 d., https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/code_conduct.pdf.

[138] Jerrold, Nadler, David N., *Cicilline, „Investigation of Competition in Digital Markets*“ (United States: 2020), Žiūrėta 2021 m. balandžio 1 d., https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.

[139] Facebook, „*Privacy policy*“, Žiūrėta 2021 m. balandžio 1 d., https://www.facebook.com/policy.php.

[140] Matthew Rosenberg, Nicholas Confessore, Carole Cadwalladr, „*How Trump Consultants Exploited the Facebook Data of Millions*“, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.

[141] Arjun Kharpal, „*Facebook shares slump amid continued fallout from Cambridge Analytica scandal*“ 2018, žiūrėta 2021 m. balandžio 19 d., https://www.cnbc.com/2018/03/19/facebook-shares-fall-over-fallout-from-cambridge-analytica-scandal.html

[142] *Facebook Reports Fourth Quarter and Full Year 2018 Results*, 2019, žiūrėta 2021 m. balandžio 19 d., https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx.

socialiniais tinklais, duomenis[143]. Tokio masto dominavimas gali būti siejamas su tuo, kad „Facebook“ taip pat kontroliuoja „Instagram“, „Messenger“ ir „WhatsApp“. Bendrovė valdo didžiąją dalį socialinių tinklų, tačiau nepaisant asmens privatumo saugumo problemų, su kuriomis susiduria „Facebook“, įmonė artimiausiu metu iš rinkos pasitraukti neketina.

Nors „Facebook“ verslo modelis JAV yra teisėtas, tačiau ES institucijos jau seniai ginčijasi su bendrove dėl duomenų apsaugos politikos[144]. Federalinės prekybos komisija prieš „Facebook“ ėmėsi veiksmų[145] JAV, tačiau komisijos galimybės ribotos, nes nėra priimta visuotinai taikomo teisės akto reguliuojančio asmenės privatumo saugą.

Pažymėtina, kad dar iki BDAR priėmimo asmens duomenų rinkimas, naudojimas ir tvarkymas buvo nepakankamai reguliuojamas. Sheila A. Millar ir Tracy P. Marshall teigimu[146], po „Cambridge Analytica“ „Facebook“ atsipirko 565 000 Eur bauda. Tai buvo tuo metu maksimali bauda, kuri skirta remiantis iki BDAR galiojusiais teisės aktais, nes pažeidimai padaryti, apie juos sužinota ir bylos nagrinėjimas pradėtas iki 2018 m. gegužės 25 d., kai visoje ES tapo privalu visa apimtimi taikyti BDAR. Tuo metu analitikai ir rinkos stebėtojai kalbėjo, kad jeigu apie pažeidimus būtų buvę pranešta įsigaliojus BDAR ir tarnyba šią netinkamo duomenų naudojimo bylą būtų pradėjusi keliais mėnesiais vėliau, būtų taikytos BDAR nuostatos. Tokiu atveju didžiausia galima bauda būtų siekusi apie 1,64 mlrd. USD (1,51 mlrd. Eur), nes „Facebook“ ankstesnių metų (2017 m.) pajamos siekė 40,6 mlrd. USD.

Nepaisant šio skandalo, 2021 m. balandžio mėn. buvo pavogta virš 500 mln. vartotojų duomenų. Atskleisti duomenys apima daugiau nei 533 milijonų „Facebook“ vartotojų iš 106 šalių asmeninę informaciją. Skelbiami vartotojų telefono numeriai, „Facebook“ ID, visi vardai, vietos, gimimo datos, biografijos duomenys ir, kai kuriais atvejais, el. pašto adresai. Nors duomenys yra 2 metų senumo, tačiau gali būti vertingi nusikaltėliams, kurie naudojasi asmenine žmonių informacija, apsimeta jais arba siekia apgauti[147]. Taigi nors „Facebook“ ne kartą mokėjo baudą dėl asmenės privatumo saugos pažeidimų, tačiau būdai gauti šiuo duomenis tampa vis įvairesni, todėl ir teisės aktai, nustatantys atsakomybę, turi būti griežtesni.

---

[143] *Social media - Statistics & Facts*, 2021, žiūrėta 2021 m. balandžio 19 d., https://www.statista.com/topics/1164/social-networks/.

[144] European Commission, „*The Privacy Shield. Update on the state of play of the EU-US data transfer rules*“, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf.

[145] Federal Trade Commission, „*FTC Sues Facebook for Illegal Monopolization*“, 2020, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization.

[146] Sheila A. Millar, Tracy P. Marshall, „What’s Next After Facebook’s Record $5 Billion Fine and Cambridge Analytica?“, *Communications, Media & Internet Consumer Protection Litigation XI(109*), 2021.

[147] Aaron Holmes, “*533 million Facebook users' phone numbers and personal data have been leaked online*”, 2021, žiūrėta 2021 m. balandžio 19 d., https://www.businessinsider.com/stolen-data-of-533-million-facebook-users-leaked-online-2021-4.

Apibendrinant galima teigti, kad „Facebook“ ne kartą demonstravo aplaidžius veiksmus užtikrinant saugumą vertingiausiam turtui - vartotojų duomenims. Bendrovė sukaupė daug duomenų, kuriuos netinkamai ir neatsakingai tvarkė, pažeisdama paslaugų teikimo taisykles, bei nepranešė socialinio tinklo vartotojams apie galimus duomenų pažeidimus. „Facebook“ verslo modelis paremtas tuo, kad šia socialinio tinklo teikiamoms paslaugos vartotojai gali naudotis nemokamai, tačiau reklamos, talpinamos platformoje – apmokestintos. Siekdama maksimaliai padidinti reklamos efektyvumą, įmonė atlieka daug darbo, susijusio su duomenų apdorojimu, kuris leidžia jiems rasti tendencijas ir efektyviai numatyti, kokio tipo turinį jų vartotojai domina. Štai kodėl bendrovė turėjo susitarimus su trečiosiomis šalimis (pvz., „Cambridge Analytica“), siekiant palengvinti atliekamų tyrimų apimtis. Trečiosios šalys tokiu būdu tobulina duomenų apdorojimo metodus ir priemones, o „Facebook“ tai naudinga, kad už juos tai atlieka profesionalūs šios srities specialistai. Tačiau, kai nuosavybės teise priklausantys „Facebook“ duomenys buvo pateikti trečiosioms šalims, „Facebook“ turėjo elgtis itin atsakingai saugant savo vartotojus ir užtikrinant, kad jų duomenys būtų saugūs. Tačiau „Cambridge Analytica“ skandalo atveju „Facebook“ laiku nepriėmė reikalingų sprendimų.

4.2. Duomenų apsaugos komisaras prieš „Facebook“ ir Maximilian Schrems

Maximillian Schrems – tai Austrijos pilietis, kuris nuo 2008 m. yra „Facebook“ socialinio tinklo vartotojas. Maximillian Schrems asmens duomenys per Airijoje esančią „Facebook“ duomenų apsaugos agentūrą siunčia socialinio tinklo duomenis į JAV teritorijoje esančius serverius, kur šie duomenys toliau yra tvarkomi. Šis Austrijos pilietis kreipėsi į Airijos priežiūros instituciją su skundu, siekiant uždrausti jo duomenų perdavimą į kitą šalį – JAV. Kaip nurodė skunde, Maximillian Schrems abejoja ar JAV teisė ir praktika pakankamai užtikrina jo duomenų apsaugą nuo teisėsaugos institucijų (pvz., nuo žvalgybos institucijų). Minėtas skundas iš pradžių buvo atmestas sprendimu 2000/520[148] (kitaip šis sprendimas vadinamasi „saugaus uosto“ sprendimas), nes Europos Komisija patikino, kad JAV esančios institucijos tinkamai tvarko duomenis, jie yra pakankamai apsaugoti. Airijos Aukštasis Teismas kreipėsi į ESTT su prejudiciniu klausimu. ESTT 2015 m. spalio 6 d. 2000/520 sprendimą pripažino negaliojančiu.

Kai ESTT pripažino 2000/250 sprendimą negaliojančiu, Airijos Aukštasis Teismas panaikino sprendimą, kuriuo buvo atmestas Maximillian Schrems skundas. Remiantis generalinio advokato Henrik

[148] Europos Sąjungos Teisingumo Teismas, „*The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid*“, 2015, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN.

Saugmandsgaard Øe išvada[149], šio Austrijos piliečio paprašyta performuluoti minėtą skundą. Naujai pateiktame skunde Maximillian Schrems prašė stabdyti duomenų apie jį perdavimą iš ES į JAV, tomis sąlygomis, kuriomis tai buvo vykdoma tuo metu, arba bent jau uždrausti šių duomenų perdavimą ateityje. Šis asmuo išreiškė nepasitikėjimą JAV teisės aktais ir esama teismų praktika, jog ji nepakankamai užtikrina jo duomenų apsaugą toje šalyje, į kurią siunčiami duomenys. Airijos priežiūros institucija padarė įžvalga, kad Maximillian Schrems skundo nagrinėjimas susijęs su „Facebook“ paslaugų teikimo standartinių apsaugos sąlygų galiojimu, todėl nurodė Airijos Aukštajam Teismui inicijuoti procesą, kad šis ESTT pateiktų prašymą priimti prejudicinį sprendimą.

Remiantis ESTT pranešimu spaudai Nr. 91/20, „po šio proceso pradėjimo Europos Komisija priėmė kitą sprendimą Nr. 2016/1250 dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo (vadinamąjį „privatumo skydo“ sprendimą). Prašymu priimti prejudicinį sprendimą šį prašymą pateikęs teismas paklausė ESTT dėl BDAR taikymo asmens duomenų perdavimui remiantis standartinėmis apsaugos sąlygomis, dėl šiuo reglamentu reikalaujamo apsaugos lygio, kai atliekamas toks perdavimas, ir dėl šiomis aplinkybėmis priežiūros institucijoms tenkančių pareigų. Be to, Airijos Aukštasis Teismas iškėlė klausimą tiek dėl sprendimo 2010/87 (dėl standartinių apsaugos sąlygų reglamentavimo), tiek dėl sprendimo 2016/1250 (dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo) galiojimo“[150].

ESTT pažymėjo[151], kad ES teisė, be kita ko, BDAR, taikoma asmens duomenų perdavimui, kurį komerciniais tikslais atlieka valstybėje narėje įsteigtas ūkio subjektas kitam trečiojoje šalyje įsteigtam ūkio subjektui, net jei atliekant šį perdavimą arba po jo atitinkamos trečiosios šalies valdžios institucijos gali tvarkyti šiuos duomenis visuomenės saugumo, gynybos ir valstybės saugumo tikslais. Jis pažymėjo jog tai, kad trečiosios šalies institucijos atlieka tokį duomenų tvarkymą, nereiškia, kad jis nepatenka į BDAR taikymo sritį. Vertinant būtiną duomenų apsaugos lygį ESTT sprendė, ar BDAR nuostatose numatytos apsaugos priemonės yra tinkamos, siekiant užtikrinti teisines ir veiksmingas asmens privatumo saugos gynimo priemones. Kitose (ne ES) šalyse, kuriose tvarkomi asmens duomenys, apsaugos lygis turi būti iš esmės lygiavertis ES garantuojamam. Atsižvelgdamas į tai, ESTT pažymėjo[152],

[149] Henrik Saugmandsgaard Øe Opinion, „*Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*“, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CC0311&qid=1414934260859.

[150] Europos Sąjungos Teisingumo Teismas, „*Teisingumo Teismas pripažino negaliojančiu Sprendimą 2016/1250dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo*“, 2020, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091lt.pdf.

[151] Europos Sąjungos Teisingumo Teismas, „*The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield*“, 2020, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[152] Europos Sąjungos Teisingumo Teismo sprendimas Byloje C-311/18 „*Dėl High Court (Aukštasis Teismas, Airija) 2018 m. gegužės 4 d. sprendimo, kurį Teisingumo Teismas gavo 2018 m. gegužės 9 d., pagal SESV 267 straipsnį pateikto prašymo*

kad užtikrinant tokio lygio apsaugą turi būti atsižvelgiama tiek į ES įsteigto duomenų valdytojo ar duomenų tvarkytojo teisinės sistemos aspektus, nurodytus BDAR 45 straipsnyje. 2 d., tiek į trečiojoje šalyje įsisteigusio duomenų gavėjo sudarytų sutarčių sąlygas.

Vertinant priežiūros institucijų atsakomybę vykdant duomenų perdavimą, ESTT pasisakė[153], kad, remiantis ES ir nacionaliniais teisės aktais (ypač BDAR 45 ir 46 str. bei Pagrindinių teisių chartijai), kompetentinga priežiūros institucija gali ir turi sustabdyti arba uždrausti duomenų perdavimą trečiajai šaliai, nebent Europos Komisija teisėtai priėmė sprendimą dėl duomenų tvarkymo ir valdymo tinkamumo patvirtintomis sąlygomis.

ESTT nagrinėjo sprendimo 2010/87 (dėl standartinių apsaugos sąlygų reglamentavimo) pagrįstumą[154]. Anot ESTT, šio sprendimo nepanaikina tai, kad jame pateiktos standartinės duomenų apsaugos sąlygos nėra privalomos trečiųjų šalių valdžios institucijoms, ir kurios gali perduoti asmens duomenis vien remiantis sutartinio pobūdžio santykiais. ESTT pažymėjo, kad sprendimo galiojimas priklauso nuo to, ar sprendime nustatyti veiksmingi mechanizmai, užtikrinantys, kad laikomasi ES teisės aktų reikalaujamo apsaugos lygio ir, kad asmens duomenų perdavimas tokiomis sąlygomis būtų sustabdytas arba uždraustas, tas sąlygas pažeidus. ESTT pasisakė, kad sprendime 2010/87 nustatyti minėti mechanizmai. ESTT be kita ko pabrėžė, kad ES veikia duomenų valdytojas, todėl perduotų asmens duomenų gavėjas privalo įsitikinti, ar atitinkamoje trečiojoje šalyje laikomasi ES teisės aktų reikalaujamo apsaugos lygio. Šių duomenų gavėjas, jei reikia, privalo informuoti duomenų valdytoją pagal šį sprendimą, jei jis negali įvykdyti standartinių apsaugos sąlygų, o tada duomenų valdytojas turi sustabdyti perdavimą ir (arba) nutraukti sutartį.

Galiausiai ESTT išnagrinėjo sprendimo 2016/1250 (dėl ES ir JAV „privatumo skydo“ suteikiamos apsaugos tinkamumo) pagrįstumą[155], atsižvelgdamas į BDAR reikalavimus pagal Europos Sąjungos pagrindinių teisių chartiją, garantuojantį teisę į privatumą ir šeimos apsaugą bei teisę į veiksmingą teisminę gynybą. Šiuo klausimu ESTT pažymėjo, kad šis sprendimas, kaip ir sprendimas 2000/520, nustatė su nacionaliniu saugumu, viešuoju interesu ir JAV įstatymų laikymusi susijusių reikalavimų viršenybę, todėl jį galima naudoti norint nustatyti asmenis, kurių asmens duomenims yra

---

priimti prejudicinį sprendimą byloje“. Eur-lex, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62018CJ0311&from=EN.

[153] Europos Sąjungos Teisingumo Teismas, „*The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield*“, 2020, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.

[154] Henrik Saugmandsgaard Øe Opinion, „*Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*“, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CC0311&qid=1414934260859.

[155] *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

taikomi trečiųjų šalių pagrindinių teisių apribojimai. ESTT pasisakė[156], kad, atsižvelgiant į tam tikras priežiūros programas, teisės aktai jokiu būdu nenurodo, kad juose yra apribojimų ar garantijų valdžios institucijoms įgyvendinti šias programas ne JAV asmenims. ESTT pridūrė, kad nors šie teisės aktai nustato reikalavimus, kurių turi laikytis JAV valdžios institucijos, įgyvendindamos atitinkamas priežiūros programas, tai duomenų valdytojams nesuteikia teisių. Kalbant apie teisminės apsaugos reikalavimą, ESTT nusprendė, kad, priešingai nei Europos Komisija konstatavo Sprendime 2016/1250, tame sprendime nurodytas ombudsmeno mechanizmas nesuteikia jiems teisių gynimo priemonės įstaigoje, teikiančioje garantijas, iš esmės lygiavertes reikalaujamoms pagal ES teisę. Pagal šį mechanizmą numatytas ombudsmeno nepriklausomumas, tiek taisyklių, įgalinančių tą ombudsmeną priimti sprendimus, privalomus JAV žvalgybos tarnyboms, egzistavimas. Dėl visų šių priežasčių ESTT paskelbė sprendimą 2016/1250 negaliojančiu.

Apibendrinant galima teigti, kad ESTT išaiškino, kad ginant žmogaus teises į privatų asmens gyvenimą, asmens duomenų perdavimą komerciniais tikslais taikomas BDAR. Šis teisės aktas taikomas ir trečiosiose šalyse įkurtoms duomenų tvarkymo ir valdymo institucijoms, nepaisant to, kad tų šalių valdžios institucijos turi teisę prieiti prie šių duomenų. BDAR nuostatos turėtų užtikrinti asmens privatumo saugą, perduodant duomenis į trečiąją šalį, remiantis standartinėmis duomenų apsaugos sąlygomis, sudarytų sutarčių sąlygomis. Europos Komisija turi teisę priimti sprendimą, kad kompetentinga priežiūros institucija sustabdytų arba uždraustų duomenų perdavimą į trečiąją šalį, jei mano, kad šioje trečiojoje šalyje šių sąlygų nesilaikoma arba jų negali laikytis.

4.3. „Fashion ID“ prieš Verbraucherzentrale

Elektroninės prekybos įmonė „Fashion ID“ į savo svetainę integravo „Facebook“ socialinį modulį „Patinka“. Kai lankytojas prisijungia prie „Fashion ID“ svetainės, to lankytojo asmeniniai duomenys perduodami „Facebook Ireland“ dėl toje svetainėje integruoto mygtuko. Toks perkėlimas vyksta be lankytojo žinios ir neatsižvelgiant į tai, ar jis yra socialinio tinklo „Facebook“ narys ar „Facebook“ paspaudė mygtuką „Patinka“[157].

Visuomeninė vartotojų teisių gynimo asociacija „Verbraucherzentrale NRW“ apkaltino „Fashion ID“, kad ši savo interneto svetainės lankytojų asmens duomenis be jų sutikimo perdavė „Facebook

[156] *Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield*, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.

[157] Opinion of Advocate General Bobek, Case C-40/17, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=FA384AD441D57FDA92F8A1F616F3E671?text=&docid=209357&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4750588.

Ireland“ ir taip pažeidė asmens duomenų apsaugos nuostatų informacijos reikalavimus. „Verbraucherzentrale NRW“ Landgericht Düsseldorf (Diuseldorfo apygardos teismas, Vokietija) pareiškė ieškinį dėl „Fashion ID“ veiksmų, siekdama nutrauktų vykdomą „Fashion ID“ veiklą. Ginčui pasiekus teismą, Oberlandesgericht Düsseldorf (Diuseldorfo aukštesnysis apygardos teismas) nutarė sustabdyti bylos nagrinėjimą ir pateikti ESTT prejudicinius klausimus[158].

Remiantis „Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams“[159], pirmuoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės klausė, ar Direktyvos 95/46 22–24 straipsniai draudžia nacionalines taisykles, leidžiančias vartotojų asociacijoms pareikšti ieškinį. ESTT pasisakė, kad tai, kad valstybė narė savo nacionalinėse taisyklėse gali vartotojų asociacijoms pareikšti ieškinį dėl asmens privatumo saugos pažeidimo, niekaip nepažeidžia Direktyvos 95/46 tikslų, priešingai, prisideda prie jų įgyvendinimo. Remiantis Direktyva 2016/679 (BDAR), kuria panaikinama ir pakeičiama Direktyva 95/46 ir, kuri galioja nuo 2018 m., gegužės 25 d., valstybėms narėms leidžiama vartotojų asociacijoms pareikšti ieškinį dėl asmens duomenų pažeidimo jokiu būdu nereiškia, kad valstybės narės negalėjo suteikti jiems šios teisės pagal Direktyvą 95/46, tačiau patvirtina, kad direktyvos aiškinimas šiame sprendimas atspindi ES įstatymų leidėjo valią.

Remiantis „Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams“[160], antruoju klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės klausė, ar interneto svetainės administratorius, „Fashion ID“, kuris toje interneto svetainėje įterpia socialinį modulį, leidžiantį šios svetainės lankytojo naršyklei prašyti minėto modulio teikėjo turinio ir perduoti šiam teikėjui lankytojo asmens duomenis, gali būti laikomas duomenų valdytoju, kaip apibrėžta Direktyvos 95/46 2 str. d p., nors tas valdytojas neturi jokios įtakos taip minėtam teikėjui perduotų duomenų tvarkymui.

ESTT pasisakė[161], kad terminas „duomenų valdytojas“ reiškia subjektą, kuris „vienas arba kartu su kitais“ nustato asmens duomenų tvarkymo tikslus ir priemones, nebūtinai nurodo vieną subjektą ir gali apimti kelis su tokiu tvarkymu susijusius subjektus, kuriems taikoma duomenų apsaugos teisės normos. Tai, kad „Fashion ID“ integravo socialinį modulį į savo svetainę, *inter alia* reiškia, kad jis turėjo lemiamą

---

[158] Opinion of Advocate General Bobek, Case C-40/17, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=FA384AD441D57FDA92F8A1F616F3E671?text=&docid=209357&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4750588.

[159] Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:l14552&from=LT.

[160] Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:l14552&from=LT.

[161] Opinion of Advocate General Bobek, Case C-40/17, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=FA384AD441D57FDA92F8A1F616F3E671?text=&docid=209357&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4750588.

poveikį tos svetainės lankytojų renkamiems ir perduotiems asmens duomenims to modulio teikėjui, šiuo atveju „Facebook Ireland“, kuris nebūtų įvykęs, jei minėtas modulis nebūtų integruotas.

Teismas pažymėjo, kad svetainėje lankėsi tiek žmonės, kurie yra socialinio tinklo „Facebook“ nariai, turintys paskyrą šiame socialiniame tinkle, tiek žmonės, neturintys tokios paskyros. Pastaruoju atveju svetainės administratoriaus „Fashion ID“ atsakomybė tvarkyti šių asmenų duomenis yra dar didesnė, nes atrodo, kad vien apsilankius svetainėje „Facebook“ mygtuko pagalba „Facebook Ireland“ pradeda tvarkyti jų asmens duomenis. Todėl „Fashion ID“ kartu su „Facebook Ireland“ gali būti laikomi atsakingais pagal Direktyvos 95/46 2 str.

Remiantis „Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams“[162], „kitu klausimu prašymą priimti prejudicinį sprendimą pateikęs teismas iš esmės klausė, ar tokioje situacijoje, kokia nagrinėjama byloje, kai interneto svetainės administratorius į minėtą svetainę integruoja socialinį modulį, leidžiantį šios svetainės lankytojo naršyklei prašyti minėto modulio teikėjo turinio ir perduoti šiam teikėjui lankytojo asmens duomenis, taikant Direktyvos 95/46 7 str. f punktą turi būti atsižvelgta į to administratoriaus teisėtą interesą arba minėto teikėjo teisėtą interesą. ESTT nuomone, kiekvienas iš šių atsakingų asmenų šiomis tvarkymo operacijomis turi siekti teisėtų interesų, kaip apibrėžta Direktyvos 95/46 7 str. f punkte, kad tokios operacijos galėtų būti pagrįstos“.

Prašymą priimti prejudicinį sprendimą pateikęs teismas siekė išsiaiškinti interneto svetainės administratoriaus pareigas gauti sutikimą tik dėl asmens duomenų tvarkymo operacijos ar operacijų rinkinio, kurių tikslus ir būdus minėtas administratorius realiai nustato. ESTT nurodė[163], kad „*kalbant apie Direktyvos 95/46 2 str. h punkte ir 7 str. a punkte nurodytą sutikimą, atrodo, kad jis turi būti duotas iki duomenų subjekto duomenų rinkimo ir perdavimo. Esant tokioms aplinkybėms, interneto svetainės administratorius, o ne socialinio modulio teikėjas turi gauti šį sutikimą, nes lankytojas apsilanko šioje interneto svetainėje, kurioje pradedamas asmens duomenų tvarkymas. Duomenų subjekto teisės nebūtų veiksmingai ir laiku apsaugotos, jei sutikimas būtų duotas tik vienam bendrai už tvarkymą atsakingam ir vėliau pradedančiam veikti subjektui, t. y. minėto modulio teikėjui. Sutikimas, kuris turi būti duotas administratoriui, yra susijęs tik su asmens duomenų tvarkymo operacija arba operacijų rinkiniu, kurių tikslus ir būdus šis administratorius realiai nustato. Vadinasi, esant tokiai situacijai, kokia nagrinėjama byloje, Direktyvos 95/46 10 str. nustatyta pareiga teikti informaciją tenka ir interneto svetainės administratoriui; vis dėlto informacija, kurią jis privalo pateikti duomenų subjektui, turi būti susijusi tik*

[162] Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:l14552&from=LT.

[163] Opinion of Advocate General Bobek, Case C-40/17, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=FA384AD441D57FDA92F8A1F616F3E671?text=&docid=209357&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4750588.

su asmens duomenų tvarkymo operacija ar operacijų rinkiniu, kurių tikslus ir būdus šis administratorius realiai nustato“.

Apibendrinant galima teigti, kad interneto svetainės administratorius, „Fashion ID“ atsakingas už tą asmens duomenų tvarkymo operaciją arba operacijų rinkinį, kurių tikslus ir būdus jis realiai nustatė, t.y. už nagrinėjamą duomenų rinkimą ir perdavimą. Esant tokiai situacijai, kokia nagrinėjama byloje, kai interneto svetainės administratorius į minėtą svetainę integruoja socialinį modulį, leidžiantį šios svetainės lankytojo naršyklei prašyti minėto modulio teikėjo turinio ir perduoti šiam teikėjui lankytojo asmens duomenis, būtina, kad ir šis administratorius, ir šis teikėjas tokiomis tvarkymo operacijomis siektų teisėtų interesų. Kai interneto svetainės administratorius integruoja į minėtą svetainę socialinį modulį, leidžiantį šios svetainės lankytojo naršyklei prašyti minėto modulio teikėjo turinio ir perduoti šiam teikėjui lankytojo asmens duomenis, šiose nuostatose nurodytą sutikimą šis administratorius privalo gauti tik dėl asmens duomenų tvarkymo operacijos ar operacijų rinkinio, kurių tikslus ir būdus minėtas administratorius realiai nustato. Taip pat numatyta pareiga pateikti informaciją tenka ir minėtam administratoriui; vis dėlto informacija, kurią jis privalo pateikti duomenų subjektui, turi būti susijusi tik su asmens duomenų tvarkymo operacija ar operacijų rinkiniu, kurių tikslus ir būdus jis realiai nustato.

Apibendrinant asmens privatumo saugos socialiniuose tinkluose įgyvendinimo problemas praktikoje nustatyta, kad socialinių tinklų valdytojai, kurių didžiausias jų „Facebook“, ne kartą demonstravo aplaidžius veiksmus užtikrinant asmens privatumo saugumą. Bendrovė kaupia daug duomenų, kuriuos tvarko nepakankamai tinkamai ir atsakingai, pažeisdama paslaugų teikimo taisykles („Cambridge Analytica“, „Fashion ID“ atvejai). Atsižvelgiant į asmens privatumo saugos socialiniuose tinkluose pažeidimų būdų įvairovę, teisės aktai užtikrinantys asmens privatumo saugą socialiniuose tinkluose yra nuolat tobulinami, todėl 2018 m. Direktyvą 95/46 keitė Europos Parlamento ir Europos Tarybos priimtas reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis (BDAR). Į BDAR taikymo sritį pateko ir asmens duomenų perdavimas trečiojoje šalyje įsteigtam ūkio subjektui. Kas nepatenka į BDAR taikymo sritį, kad asmenų duomenimis gali naudotis trečiosios šalies valdžios institucijos. Taip pat nustatyta, kad asmens duomenų apsaugą užtikrina įvairūs tarptautiniai ir nacionaliniai teisės aktai, tačiau asmens duomenų apsauga vyksta ne tik per supranacionalinį teisinį reglamentavimą, o ir ESTT plėtojamą jurisprudenciją.

IŠVADOS IR PASIŪLYMAI

1. Asmens privatus gyvenimas ne tik jo asmeninė, nuošali erdvė, į kurią neturi teisės ir nesikiša tretieji asmenys, tačiau tai ir žmogaus santykiai su socialine aplinka, informacija apie jį, asmenybės teisių visumos apsauga. Asmens teisės į privatumą turinį sudaro keturi savarankiški, tarpusavyje susiję privataus gyvenimo požymiai: fizinis, komunikacinis, teritorinis ir informacinis privatumas. Europos žmogaus teisių teismas pateikė privataus gyvenimo sampratą ir jo turinį, o Lietuvos Respublikos Konstitucinis Teismas pažodžiui perėmė šio teismo doktriną. Asmens teisė į privatumą nėra absoliuti ir, remiantis tarptautiniais ir nacionaliniai teisės aktais, valstybinės institucijos neturi teisės riboti asmenes teisės į privatų gyvenimą, išskyrus atvejus, įtvirtintus EŽTK 8 str. 2 d., bei įstatymų nustatyta tvarka, siekiant užtikrinti valstybės saugumą, visuomenės sveikatos apsaugą, ginant šalies ekonominės gerovės interesus, užkertant kelią viešosios tvarkos pažeidimams ir nusikaltimams, ginant asmenų teisių ir laisvių visetą.
2. Asmens teisė į privatumą tarptautiniuose teisės aktuose pradėta reguliuoti neseniai, tačiau esamas reguliavimas pakankamas. Asmens teisė į privatų gyvenimą, asmenų duomenų apsaugą garantuoja Konvencija Nr. 108 „Dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu“, Europos žmogaus teisių konvencija, Europos Sąjungos pagrindinių teisių chartija, Tarptautinis pilietinių ir politinių teisių paktas. Europos Sąjungos lygmeniu priimta eilė direktyvų, tačiau pagrindinė jų – Bendrasis duomenų apsaugos reglamentas, kuris taikomas visose ES valstybėse narėse nuo 2018 m. gegužės 25 d. Bendrasis duomenų apsaugos reglamentas užtikrina piliečių teises: dėl aiškaus sutikimo tvarkyti jų duomenis, dėl teisės būti pamirštam, dėl teisės perduoti duomenis kitam paslaugų tiekėjui, dėl teisės žinoti, kada privatumo sauga buvo pažeista. Naujosios taisyklės taikomos visoms ES veikiančioms įmonėms, net ir toms, kurios įsikūrusios už jos ribų. Be to, įmonėms, kurios pažeidžia taisykles taikomos priemonės: įspėjimai arba baudos. Lietuvos Respublikoje kuriami ir tobulinami asmens teisės į privatumą teisinio reguliavimo pagrindai. Nacionaliniai teisės aktai reguliuojantys asmens teisės į privatumą apima įvairias gyvenimo sritis, įvairaus amžiaus grupių asmenis, todėl galima daryti išvadą, kad teisinis reglamentavimas yra pakankamas.
3. Šių dienų asmens privatumas socialiniuose tinkluose apima vartotojų patirtį, nuomones ir žinias, asmeninius duomenis, pvz., vardą, lytį, buvimo vietą ir privačias nuotraukas (vaizdo įrašus). Socialinių tinklų naudojami įrankiai (būsenos atnaujinamas socialiniame tinkle, privačių asmens duomenų dalijimasis su trečiosiomis šalimis, aplikacijų programavimo sąsaja, paieškos sistemos, vietos duomenys) pakeitė vartotojų sąveiką asmeniniame ir profesiniame gyvenime, bei tačiau tuo

pačiu kelia ir didelę riziką, susijusią su asmens privatumu ir saugumu. Pagrindiniai asmens privatumo saugos socialiniuose tinkluose pažeidimo būdai yra: socialinės inžinerijos ir atvirkštinės socialinės inžinerijos atakos, tapatybės vagystės, šlamšto atakos, kenkėjiškų programų diegimas ir kt. Užtikrinant asmens privatumo saugą socialiniuose tinkluose susiduriama su trimis pagrindinėmis problemomis: privatumas, vientisumas ir prieinamumas. Socialinių tinklų inžinieriai turėtų siekti ne tik apsaugoti vartotojų asmeninę informaciją ir turinį, kuriuo jie dalijasi savo sienoje, profilyje, bet ir siekiama, kad socialinių tinklų narių naudojami komunikacijos kanalai būtų apsaugoti nuo vidinių ar išorinių išpuolių, kad trečiosios šalies vartotojai negalėtų patekti į juos. Taip pat siekiama užkirsti kelią trečiosioms šalims sužinoti, kurie vartotojai tarpusavyje bendrauja. Galiausiai, turi būti įdiegti prieigos kontrolės mechanizmai, užtikrinant, kad turinys būtų prieinamas vartotojams, kuriems buvo suteiktas leidimas pasiekti tokį turinį.

4. Išanalizavus asmens privatumo saugos socialiniuose tinkluose įgyvendinimo problemas praktikoje nustatyta, kad socialinių tinklų valdytojai, kurių didžiausias jų „Facebook“, ne kartą demonstravo aplaidžius veiksmus užtikrinant asmens privatumo saugumą. Bendrovė kaupia daug duomenų, kuriuos tvarko nepakankamai tinkamai ir atsakingai, pažeisdama paslaugų teikimo taisykles („Cambridge Analytica“, „Fashion ID“ atvejai). Atsižvelgiant į asmens privatumo saugos socialiniuose tinkluose pažeidimų būdų įvairovę, teisės aktai užtikrinantys asmens privatumo saugą socialiniuose tinkluose yra nuolat tobulinami, todėl 2018 m. Direktyvą 95/46 keitė Europos Parlamento ir Europos Tarybos priimtas reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis (BDAR). Į BDAR taikymo sritį pateko ir asmens duomenų perdavimas trečiojoje šalyje įsteigtam ūkio subjektui. Kas nepatenka į BDAR taikymo sritį, kad asmenų duomenimis gali naudotis trečiosios šalies valdžios institucijos. Taip pat nustatyta, kad asmens duomenų apsaugą užtikrina įvairūs tarptautiniai ir nacionaliniai teisės aktai, tačiau asmens duomenų apsauga vyksta ne tik per supranacionalinį teisinį reglamentavimą, o ir ESTT plėtojamą jurisprudenciją.

LITERATŪROS SĄRAŠAS

Monografijos ir straipsnių rinkiniai:

1. Beye, Michael et al., *Literature Overview - Privacy in Online Social Networks", Computational Social Networks*. Springer, 2012.
2. Deliri, Sepideh, Albanese, Massimiliano. „*Security and Privacy Issues in Social Networks*". Data Management in Pervasive Systems. Cham: Springer, 2015.
3. Jočienė, Danutė, Čilinskas, Kęstutis. *Žmogaus teisių apsaugos problemos tarptautinėje ir Lietuvos Respublikos teisėje*. Vilnius: UAB „Petro ofsetas", 2004.
4. Lietuvos Respublikos Konstitucijos komentaras (I dalis). Vilnius: Teisės institutas, K. Jovaišo PĮ, 2000.
5. Pumputis, Alvydas ir kt., *Kontitucingumas ir pilietinė visuomenė*. Vilnius: Lietuvos teisės universiteto Leidybos centras, 2002.

Moksliniai straipsniai ir darbai:

6. Abel, Lamidi Dare, Makun, Gana, Benjamin, Alafiatayo. „*Use of Social Media in Information Dissemination*", 2014, žiūrėta 2021 m. vasario 1 d., https://www.researchgate.net/publication/319230692_Use_of_Social_Media_in_Information_Dissemination.
7. Ahmad, Ali, Kamran, Ahmad, Mansoor, Malik, Basit Raza, Ahmed. „Privacy Concerns in Online Social Networks: A Users' Perspective", *International Journal of Advanced Computer Science and Applications 10*, 7 (2019).
8. Baltassis, Elias, Rose, John, Gourevitch, Antoine. „*Leveraging GDPR to become a trusted data steward, The Boston Consulting Group*", 2020, žiūrėta 2020 m. rugsėjo 1 d., https://www.bcg.com/en-us/publications/2018/leveraging-gdpr-be-come-trusted-data-steward.aspx.
9. Boyd, Dahan, Ellison, Nicole, „*Social network sites: definition, history, and scholarship". Journal of computer-mediated communication*, 13 (2007), žiūrėta 2021 m. vasario 1 d., https://academic.oup.com/jcmc/article/13/1/210/4583062.
10. Cadwalladr, Carole. „*I created Steve Bannon's psychological warfare tool': meet the data war whistleblower*", The Cambridge Analytica Files, 2018, Žiūrėta 2021 m. balandžio 1 d., http://www.hec.unil.ch/lspinto/Papers%20&%20CV/The%20Cambridge%20Analytica%20Files.pdf.

11. Civilka, Mindaugas, Šlapimaitė, Lina. „Asmens duomenų samprata elektroninėje erdvėje“, *Teisė 96*, (2015): 126 – 148.
12. Colace, Francesco, Massimo, De Santo, Moscato, Vincenzo, Picariello, Antonio, Schreiber, Fabio Letizia, „*Data Management in Pervasive Systems*“, Žiūrėta 2021 m. balandžio 1 d., https://link.springer.com/book/10.1007%2F978-3-319-20062-0.
13. Committee on Energy and Commerce, „*Hearing before the Committee on Energy nad Commerce House of Representatives. One hundred fifteen Congress. Second Session. Facebook transparency and use of consumer data*“, žiūrėta 2021 m. balandžio 19 d., https://www.govinfo.gov/content/pkg/CHRG-115hhrg30956/pdf/CHRG-115hhrg30956.pdf.
14. Craft, Mary. „*Big data, little privacy: protecting consumers' data while promoting economic growth*”, Žiūrėta 2021 m. balandžio 1 d., https://www.reminger.com/media/publication/15075_BIG%20DATA%20LITTLE%20PRIVACY%20PROTECTING%20CONSUMERS%20DATA%20WHILE%20PROMOTING%20ECONOMIC%20GROWTH.pdf
15. Davis, Harry, „*Ted Cruz using firm that harvested data on millions of unwitting Facebook users*“, 2015, žiūrėta 2021 m. balandžio 19 d., https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
16. DeCapua, Todd. „*How a software bug slammed Facebook users*“, žiūrėta 2021 m. balandžio 19 d., https://techbeacon.com/app-dev-testing/how-software-bug-slammed-facebook-users.
17. Edelson, Josh, „*A timeline of Facebook's privacy issues and its responses*“, NBC News, žiūrėta 2020 m. rugsėjo 1 d., https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-re-sponses-n859651.
18. Edosomwan, Simeon, Prakasan, Sitalaskshmi, Kouame, Doriane, Watson, Jonelle, Seymour, Tom. „The History of Social Media and its Impact on Business“. *The Journal of Applied Management and Entrepreneurship, 16* (2011).
19. Emmet, Dave. „*Taxonomy of Social Networks*“, 2019, žiūrėta 2021 m. vasario 7 d., https://davemmett.wordpress.com/2009/06/15/taxonomy-of-social-networks/.
20. *Facebook Reports Fourth Quarter and Full Year 2018 Results*, 2019, žiūrėta 2021 m. balandžio 19 d., https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx.
21. Facebook. „*Code of Conduct*“, Žiūrėta 2021 m. balandžio 1 d., https://s21.q4cdn.com/399680738/files/doc_downloads/governance_documents/code_conduct.pdf.
22. Facebook. „*Privacy policy*“, Žiūrėta 2021 m. balandžio 1 d., https://www.facebook.com/policy.php.

23. Federal Trade Commission. „*FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*“, 2019, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
24. Federal Trade Commission. „*FTC Sues Facebook for Illegal Monopolization*“, 2020, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization.
25. Federal Trade Commission., „*Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*“, 2011, žiūrėta 2021 m. balandžio 19 d., https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.
26. Frauenstein, Edwin Donald, Flowerday, Stephen. „Susceptibility to phishing on social network sites: A personality information processing model“, *Computers & Security 94* (2020).
27. Gubbs, D. Amelia. „*Privacy Law and the Internet using Facebook.com as a Case Study Study*“. Chancellor’s Honors Program Projects (2011), žiūrėta 2021 m. balandžio 19 d., https://trace.tennessee.edu/cgi/viewcontent.cgi?article=2397&context=utk_chanhonoproj.
28. Hinds, Joanne, Williams, Emma J., Joinson, Adam N. „It wouldn't happen to me: Privacy concerns and perspectives following the Cambridge Analytica scandal“. *International Journal of Human-Computer Studies 143* (2020).
29. Houser, Kimberly, Voss, W. Gregory. „GDPR: The End of Google and Facebook or a New Paradigm in Data Privacy?“, *SSRN Electronic Journal*, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.researchgate.net/publication/326755233_GDPR_The_End_of_Google_and_Facebook_or_a_New_Paradigm_in_Data_Privacy.
30. Jang-Jaccard, Julian, Nepal, Surya. „A survey of emerging threats in cybersecurity“, *Journal of Computer and System Sciences 80*(5) 2014.
31. Kharpal, Arjun. „*Facebook shares slump amid continued fallout from Cambridge Analytica scandal*“ 2018, žiūrėta 2021 m. balandžio 19 d., https://www.cnbc.com/2018/03/19/facebook-shares-fall-over-fallout-from-cambridge-analytica-scandal.html.
32. Kolt, Noam. „Return on Data: Personalizing Consumer Guidance in Data Exchanges“, *Yale Law & Policy Review, 38* (77) 2019.
33. Kosinski, Michael, Stillwell, David. „*Digital records could expose intimate details and personality traits of millions*“, 2013, žiūrėta 2021 m. balandžio 19 d., https://www.cam.ac.uk/research/news/digital-records-could-expose-intimate-details-and-personality-traits-of-millions.

34. Kozlowska, Iga. „*Facebook and Data Privacy in the Age of Cambridge Analytica" (Washington: University of Washington*, 2018, Žiūrėta 2021 m. balandžio 19 d., https://jsis.washington.edu/news/facebook-data-privacy-age-cambridge-analytica/.
35. Loftsgordon, Amy. „*Social Media and Your Privacy Rights*", 2021, žiūrėta 2021 m. vasario 1 d., https://www.nolo.com/legal-encyclopedia/social-media-and-your-privacy-rights.html.
36. Lunn, Bernanrd, „*Social Network Types, Motivations, and the Future*", 2017, žiūrėta 2021 m. vasario 7 d., https://readwrite.com/2007/09/12/social_network_types_motivations/.
37. Malinauskaitė, Inga. „Privatumas virtualiuose socialiniuose tinkluose kaip įstatymo saugoma vertybė", *Social Transformations in Contemporary Society 3,* (2015).
38. *Mark Zuckerberg's Wednesday testimony to Congress on Cambridge Analytica*, Žiūrėta 2021 m. balandžio 1 d., https://www.politico.com/story/2018/04/09/transcript-mark-zuckerberg-testi
39. Meškauskaitė, Liudvika, Lankauskas, Mindaugas. „Baudžiamoji atsakomybė už asmens privataus gyvenimo neliečiamumo pažeidimus Europos žmogaus teisių teismo bei Lietuvos teismų praktikos kontekste", *Teisės problemos 1,* 91 (2016): 52 – 80.
40. Millar, Sheila, Marshall, Tracy. „What's Next After Facebook's Record $5 Billion Fine and Cambridge Analytica?", *Communications, Media & Internet Consumer Protection Litigation XI*(109), 2021.
41. Mousavi, Reza, Chen, Rui, Kim, Dan J. Kuanchin Chen, „Effectiveness of privacy assurance mechanisms in users' privacy protectionon social networking sites from the perspective of protection motivation theory", *Decision Support Systems 135* (2020): 1–14.
42. Nadler, Jerrold, Cicilline, David. „*Investigation of Competition in Digital Markets*" (United States: 2020), Žiūrėta 2021 m. balandžio 1 d., https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf?utm_campaign=4493-519.
43. Nahier, Aldhafferi, Charles, Watson, Adam, Sajje. „Personal information privacy settings of online social networks and their suitability for mobile internet device". *International Journal of Security, Privacy and Trust Management, 2* (2013).
44. Nenadic, Iva, „Unpacking the „European approach" to tackling challenges of disinformation andpolitical manipulation", *Internet policy review, 8*(4) 2019.
45. Newcomb, Alyssa, „*A timeline of Facebook's privacy issues and its responses*", NBC News, žiūrėta 2020 m. rugsėjo 1 d., https://www.nbcnews.com/tech/social-media/timeline-facebook-s-privacy-issues-its-responses-n859651.

46. Petraitytė, Ilona, „*Asmens duomenų teisinės apsaugos principai*“, Daktaro disertacija. Socialiniai mokslai, teisė (01S). Vilnius: Vilniaus universitetas, 2013.
47. Petterson, Dan, „*Facebook data privacy scandal: A cheat sheet*“, Žiūrėta 2021 m. balandžio 1 d., https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/.
48. Razmaitė, Toma, „Google street view” atvejis: teisės į privatumą ir technologijų plėtros santykis“. Vilnius: MRU, 2014.
49. Romansky, Radi, „Social media and personal data protection*“, International Journal on Information Technologies & Security, 4* (2014): 65–80.
50. Rosenberg, Matthew, Confessore, Nicholas, Cadwalladr, Carole. „*How Trump Consultants Exploited the Facebook Data of Millions*“, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
51. Segall, Jordan E. „Google Street View: Walking the Line of Privacy –Intrusion upon Seclusion and Publicity Given to Private Facts in the Digital Age“, *Pittsburgh Journal of Technology Law and Policy, 1*, 14 (2010).
52. Sfetcu, Nicolae. „*Web 2.0 / Social media / Social networks*“. 2017, žiūrėta 2021 m. vasario 1 d., https://www.researchgate.net/publication/338345786_Web_20_Social_Media_Social_Networks.
53. *Social media - Statistics & Facts*, 2021, žiūrėta 2021 m. balandžio 19 d., https://www.statista.com/topics/1164/social-networks/.
54. Sundaram, Ajith. „Understanding and Protecting Yourself against Threats in the Internet“, *Asian Social Science 13*,12 (2017).
55. Sushama, Carl, Kumar, Sunil, Neelima, Paul. „ Privacy and security issues in the future: A social media. Materials Today“, *Proceedings 1*,7 (2002).
56. Tulane University, „*Key Social Media Privacy Issues for 2020*“, 2021, žiūrėta 2021 m. balandžio 19 d., https://sopa.tulane.edu/blog/key-social-media-privacy-issues-2020.
57. University of Warwick. „*Targeted Facebook ads shown to be highly effective in the 2016 US Presidential election*.” ScienceDaily, žiūrėta 2021 m. balandžio 19 d., www.sciencedaily.com/releases/2018/10/181025103303.htm.
58. Waldman, Ari Ezra. „*Privacy, Sharing, and Trust: The Facebook Study*“, Žiūrėta 2021 m. balandžio 1 d., https://scholarlycommons.law.case.edu/cgi/viewcontent.cgi?article=4679&context=caselrev.
59. White, Mary Gormandy. „*What Types of Social Networks Exist*?“. 2021, žiūrėta 2021 m. vasario 7 d., https://socialnetworking.lovetoknow.com/What_Types_of_Social_Networks_Exist.

60. Wilhelm, Ernst Oliver. „*A brief History of the General Data Protection Regulation*“, 2016, žiūrėta 2020 m. rugsėjo 17 d. <https://iapp.org/resources/article/a-brief-history-of-the-general-data-protection-regulation/>.
61. Wong, Julia Carrie. „*Document reveals how Facebook downplayed early Cambridge Analytica concerns*“, 2019, Žiūrėta 2021 m. balandžio 1 d., https://www.theguardian.com/technology/2019/aug/23/cambridge-analytica-facebook-response-internal-document.
62. Zhenhui, Jiang, Suang Heng, Cheng, Ben CF Choi. „Research note – privacy concerns and privacy – protective behavior in synchronous online social interactions“, *Information Systems Research 24*, (2013): 579–595.
63. Zuckerberg, Mark. „*A Privacy-Focused Vision for Social Networking*“, žiūrėta 2021 m. balandžio 19 d., https://www.facebook.com/notes/2420600258234172/.
64. Žiobienė, Edita. „Aktualios konstitucinės teisės į privatų gyvenimą apsaugos problemos“, *Jurisprudencija, 64* (2005).

Tarptautinės sutartys ir kiti dokumentai:

65. „Europos Tarybos Generalinė Asamblėjos rezoliucija Nr. 428/1970 „Dėl masinės informacijos priemonių“ žiūrėta 2020 m. lapkričio 1 d/. http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=15842&lang=en.
66. „Europos žmogaus teisių ir pagrindinių laisvių apsaugos konvencija“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.19841.
67. „Tarptautinis pilietinių ir politinių teisių paktas“, LRS, žiūrėta 2021 m. vasario 2 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.174848,
68. „Visuotinė žmogaus teisių deklaracija“, LRS, Žiūrėta 2020 m. spalio 31 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278385.

Tarptautinių teismų praktika:

69. Europos Sąjungos Teisingumo Teismas, „Teisingumo Teismas pripažino negaliojančiu Sprendimą 2016/1250dėl ES ir JAV „privatumo skydo“ užtikrinamos apsaugos tinkamumo“, 2020, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091lt.pdf.

70. Europos Sąjungos Teisingumo Teismas, „The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid", 2015, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62014CJ0362&from=EN.
71. Europos Sąjungos Teisingumo Teismas, „The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield", 2020, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf.
72. Europos Sąjungos Teisingumo Teismo sprendimas Byloje C-311/18 „Dėl High Court (Aukštasis Teismas, Airija) 2018 m. gegužės 4 d. sprendimo, kurį Teisingumo Teismas gavo 2018 m. gegužės 9 d., pagal SESV 267 straipsnį pateikto prašymo priimti prejudicinį sprendimą byloje". Eur-lex, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62018CJ0311&from=EN.
73. Niemietz prieš Vokietiją, Application No. 13710/88. 1992.
74. Opinion of Advocate General Bobek, Case C-40/17, žiūrėta 2021 m. balandžio 19 d., https://curia.europa.eu/juris/document/document.jsf;jsessionid=FA384AD441D57FDA92F8A1F616F3E671?text=&docid=209357&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4750588.
75. Peck prieš Jungtinę Karalystę, Application No. 44647/98. 2003.
76. Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:l14552&from=LT.
77. Prejudicinio sprendimo priėmimo procedūra: rekomendacijos nacionaliniams teismams, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=LEGISSUM:l14552&from=LT.
78. Pretty prieš Jungtinę Karalystę, Application No. 2346/02. 2002.
79. X ir Y prieš Nyderlandus, Application No. 8978/80. 1985.

ES teisės aktai:

80. „Europos Parlamentas ir Tarybos direktyva „Dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (95/46/EB)", Eur-lex, Žiūrėta 2020 m. lapkričio 1 d., http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:LT:NOT.
81. „Europos Sąjungos pagrindinių teisių chartija", Eur-lex, , žiūrėta 2020 m. spalio 27 d., https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=FR.

82. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL L 119, 2016 5 4, p. 1–88.
83. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG.
84. European Commission, „The Privacy Shield. Update on the state of play of the EU-US data transfer rules“, 2018, žiūrėta 2021 m. balandžio 19 d., https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/625151/EPRS_IDA(2018)625151_EN.pdf.
85. Europos Komisija. 2012 m. sausio 25 d. Pasiūlymas dėl Europos Parlamento ir Tarybos reglamento dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (Bendrasis duomenų apsaugos reglamentas), KOM(2012) 11 galutinis, Briuselis.
86. Henrik Saugmandsgaard Øe Opinion, „Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems“, žiūrėta 2021 m. balandžio 19 d., https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62018CC0311&qid=1414934260859.

Lietuvos Respublikos teisės aktai:

87. „Lietuvos Respublikos advokatūros įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.229789?jf.
88. „Lietuvos Respublikos baudžiamasis kodeksas“, TAR, Žiūrėta 2020 m. lapkričio 1 d.,
89. „Lietuvos Respublikos elektroninių ryšių įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.232036/RKktjkmTCK.
90. „Lietuvos Respublikos nepilnamečių apsaugos nuo neigiamo viešosios informacijos poveikio įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.183129/OEFZHiiLcf.
91. „Lietuvos Respublikos pacientų teisių ir žalos sveikatai atlyginimo įstatymas“, LRS, žiūrėta 2020 m. rugsėjo 17 d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.31932?jfwid=32wf94v5.
92. „Lietuvos Respublikos visuomenės informavimo įstatymas“, TAR, žiūrėta 2020 m. rugsėjo 17 d., https://www.e-tar.lt/portal/lt/legalAct/TAR.065AB8483E1E/asr.

Lietuvos Respublikos teismų praktika:

93. „Lietuvos Respublikos Konstitucinio Teismo 1999 m. spalio 21d. nutarimas Nr. 90-2662 „Dėl Lietuvos Respublikos Aukščiausiosios tarybos 1991 m. sausio 31 d. nutarimo „Dėl vardų ir pavardžių rašymo Lietuvos Respublikos piliečio pase" atitikimo Lietuvos Respublikos Konstitucijai", LRKT, žiūrėta 2020 m. lapkričio 1 d.,
94. „Lietuvos Respublikos Konstitucinio Teismo 2003 m. kovo 24 d. nutarimas dėl Lietuvos Respublikos pataisos darbų kodekso 41 straipsnio 2 dalies (1997 m. liepos 2 d. redakcija) atitikties Lietuvos Respublikos Konstitucijai", LRKT, Žiūrėta 2020 m. lapkričio 1 d., http://www.lrkt.lt/dokumentai/2003/n030324.htm>.
95. „LR Konstitucinio Teismo 2000 m. birželio 30 d. nutartis Nr. 30/98-13/99 „Dėl Lietuvos Respublikos žalos, padarytos neteisėtais kvotos, tardymo, prokuratūros ir teismo veiksmais, atlyginimo įstatymo 3 str. 1 d. ir 4 str. 1 d. 1 p. atitikimo LR Konstitucijai", LRKT, žiūrėta 2020 m. rugsėjo 17 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta343/content.
96. Lietuvos Respublikos Konstitucinio Teismo nutarimas „Dėl Telekomunikacijų, Operatyvinės veiklos įstatymų ir Baudžiamojo proceso kodekso", LRKT, Žiūrėta 2020 m. lapkričio 1 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta309/content.
97. Lietuvos Respublikos Konstitucinio Teismo nutarimas „Dėl viešojo asmens privataus gyvenimo apsaugos ir žurnalisto teisės neatskleisti informacijos šaltinio", LRKT, Žiūrėta 2020 m. lapkričio 1 d., https://www.lrkt.lt/lt/teismo-aktai/paieska/135/ta311/content.

ANOTACIJA

Remiantis mokslinės literatūros, teisės aktų analize, darbe nagrinėjama asmens privatumo saugos socialiniuose tinkluose teisinio reguliavimo problematika. Magistro darbe pateikiami teisės į privatų gyvenimą koncepcijos probleminiai aspektai, analizuojant teisės į privatų gyvenimą sampratą, turinį, privatumo ribas, asmens privatumo užtikrinimo principus ir priemones. Taip pat darbe pristatoma asmens privatumo saugos tarptautinio ir nacionalinio teisinio reguliavimo raida ir probleminiai aspektai. Magistro darbe analizuojami asmens privatumo saugos socialiniuose tinkluose pažeidimo ir užtikrinimo būdai, analizuojama teismų praktika. Išnagrinėjus asmens privatumo saugos socialiniuose tinkluose įgyvendinimo problemas praktikoje nustatyta, kad socialinių tinklų valdytojai, kurių didžiausias jų „Facebook“, ne kartą demonstravo aplaidžius veiksmus užtikrinant asmens privatumo saugumą. Atsižvelgiant į asmens privatumo saugos socialiniuose tinkluose pažeidimų būdų įvairovę, teisės aktai užtikrinantys asmens privatumo saugą socialiniuose tinkluose yra nuolat tobulinami, todėl 2018 m. Direktyvą 95/46 keitė Europos Parlamento ir Europos Tarybos priimtas reglamentas 2016/679 (BDAR). Nustatyta, kad asmens duomenų apsaugą užtikrina įvairūs tarptautiniai ir nacionaliniai teisės aktai, tačiau asmens duomenų apsauga vyksta ne tik per supranacionalinį teisinį reglamentavimą, o ir ESTT plėtojamą jurisprudenciją.

ANNOTATION

Based on the scientific literature and legal acts analysis, examined personal privacy safety in social networks regulation issues. In the master’s thesis studied problematic aspects of the private life right concept, analyzed the content of private life right, privacy limits, principles and means of ensuring personal privacy. The study also presented personal privacy protection problematic aspects in international and national legal regulation. In the master’s thesis analyzed case law of personal privacy security violating ways in social networks. Personal privacy protection in social networks case study revealed, that social network managers, the largest of whom is Facebook, have repeatedly demonstrated negligent actions in ensuring the security of personal privacy. Regarding to personal privacy protection in social networks violations variety, the legislation guaranteeing personal privacy protection in social networks are constantly under development, so in 2018 Directive 95/46 was amended by Directive 2016/679 (GDPR) adopted by the European Parliament and the Council of Europe. Although the personal data protection is guaranteed by various international and national legal acts, the protection of personal data takes place not only through supranational legal regulation, but also through the jurisprudence developed by the ECJ.

SANTRAUKA

Raktiniai žodžiai: asmens privatumo sauga, socialiniai tinklai, asmens privatumo sauga socialiniuose tinkluose.

Remiantis mokslinės literatūros, teisės aktų analize, darbe analizuojama asmens privatumo saugos socialiniuose tinkluose teisinio reguliavimo problematika. Magistro darbe pateikiami teisės į privatų gyvenimą koncepcijos probleminiai aspektai, analizuojant teisės į privatų gyvenimą sampratą, turinį, privatumo ribas, asmens privatumo užtikrinimo principus ir priemones. Taip pat darbe pristatoma asmens privatumo saugos tarptautinio ir nacionalinio teisinio reguliavimo raida ir probleminiai aspektai. Magistro darbe analizuojami asmens privatumo saugos socialiniuose tinkluose pažeidimo ir užtikrinimo būdai, analizuojama teismų praktika, kurioje ginamas asmens privatumas socialiniuose tinkluose.

Šių dienų asmens privatumas socialiniuose tinkluose apima vartotojų patirtį, nuomones ir žinias, asmeninius duomenis, pvz., vardą, lytį, buvimo vietą ir privačias nuotraukas (vaizdo įrašus). Socialinių tinklų naudojami įrankiai (būsenos atnaujinamas socialiniame tinkle, privačių asmens duomenų dalijimasis su trečiosiomis šalimis, aplikacijų programavimo sąsaja, paieškos sistemos, vietos duomenys) pakeitė vartotojų sąveiką asmeniniame ir profesiniame gyvenime, bei tačiau tuo pačiu kelia ir didelę riziką, susijusią su asmens privatumu ir saugumu. Pagrindiniai asmens privatumo saugos socialiniuose tinkluose pažeidimo būdai yra: socialinės inžinerijos ir atvirkštinės socialinės inžinerijos atakos, tapatybės vagystės, šlamšto atakos, kenkėjiškų programų diegimas ir kt. Socialinių tinklų inžinieriai turėtų siekti ne tik apsaugoti vartotojų asmeninę informaciją ir turinį, kuriuo jie dalijasi savo sienoje, profilyje, bet ir siekiama, kad socialinių tinklų narių naudojami komunikacijos kanalai būtų apsaugoti nuo vidinių ar išorinių išpuolių, kad trečiosios šalies vartotojai negalėtų patekti į juos. Taip pat siekiama užkirsti kelią trečiosioms šalims sužinoti, kurie vartotojai tarpusavyje bendrauja.

Išnagrinėjus asmens privatumo saugos socialiniuose tinkluose įgyvendinimo problemas praktikoje nustatyta, kad socialinių tinklų valdytojai, kurių didžiausias jų „Facebook“, ne kartą demonstravo aplaidžius veiksmus užtikrinant asmens privatumo saugumą. Atsižvelgiant į asmens privatumo saugos socialiniuose tinkluose pažeidimų būdų įvairovę, teisės aktai užtikrinantys asmens privatumo saugą socialiniuose tinkluose yra nuolat tobulinami, todėl 2018 m. Direktyvą 95/46 keitė Europos Parlamento ir Europos Tarybos priimtas reglamentas 2016/679 (BDAR). Nustatyta, kad asmens duomenų apsaugą užtikrina įvairūs tarptautiniai ir nacionaliniai teisės aktai, tačiau asmens duomenų apsauga vyksta ne tik per supranacionalinį teisinį reglamentavimą, o ir ESTT plėtojamą jurisprudenciją.

SUMMARY

Keywords: personal privacy protection, social networks, personal privacy protection in social networks.

Based on the scientific literature and legal acts analysis, examined personal privacy safety in social networks regulation issues. In the master's thesis studied problematic aspects of the private life right concept, analyzed the content of private life right, privacy limits, principles and means of ensuring personal privacy. The study also presented personal privacy protection problematic aspects in international and national legal regulation. In the master's thesis analyzed case law of personal privacy security violating ways in social networks.

Today's personal privacy in social networks includes user experience, opinions and knowledge, personal data such as name, gender, location, and private photos (videos). The tools used by social networks (status updates on the social network, sharing of private personal data with third parties, application programming interface, search engines, local data) have changed user interactions in personal and professional life, but also pose significant risks to personal privacy and security. The main ways of violating the security of personal privacy in social networks are social engineering and reverse social engineering attacks, identity theft, spam attacks, malware installation, etc. Social network engineers should not only aim to protect users' personal information and content they share, but also to protect the communication channels used by social network members from internal or external attacks to prevent third-party users from accessing them. It also aims to prevent third parties from finding out which users are interacting with each other.

Personal privacy protection in social networks case study revealed, that social network managers, the largest of whom is Facebook, have repeatedly demonstrated negligent actions in ensuring the security of personal privacy. Regarding to personal privacy protection in social networks violations variety, the legislation guaranteeing personal privacy protection in social networks are constantly under development, so in 2018 Directive 95/46 was amended by Directive 2016/679 (GDPR) adopted by the European Parliament and the Council of Europe. Although the personal data protection is guaranteed by various international and national legal acts, the protection of personal data takes place not only through supranational legal regulation, but also through the jurisprudence developed by the ECJ.

PATVIRTINIMAS APIE ATLIKO DARBO SAVARANKIŠKUMĄ

2021 m. balandžio 19 d.
Kaunas

Aš, Mykolo Romerio universiteto (toliau – Universitetas), Viešojo saugumo akademijos, Teisės ir policijos veiklos programos studentas Lindas Judžentas, patvirtinu, kad šis bakalauro baigiamasis darbas

„SOCIALINIAI TINKLAI IR ASMENS PRIVATUMO SAUGA“

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

Linas Judžentas