Vilniaus universiteto Teisės fakulteto
Privatinės teisės katedra

Justės Mažeikaitės
V kurso, komercinės teisės
studijų šakos studentės

Magistro darbas

Asmens duomenų rinkimas ir naudojimas elektroninėje erdvėje: probleminiai aspektai

Vadovas: lekt. dr. Stasys Drazdauskas

Recenzentas: lekt. Gintautas Bartkus

Vilnius
2017

TURINYS

ĮVADAS

Temos aktualumas. Teisę į asmens duomenų apsaugą įtvirtina Europos Sąjungos pagrindinių teisių chartijos[1] 8 straipsnis. Šis straipsnis ne tik *expressis verbis* nurodo tokią teisę, bet ir pateikia pagrindinius asmens duomenų tvarkymo ir naudojimo principus: tikslingumą bei asmens sutikimo ar kito teisėto tvarkymo pagrindo būtinumą. Tinkamas šių principų įgyvendinimas turi neabejotiną įtaką asmens privačiam gyvenimui[2]. Pastaruoju metu su elektronine erdve susiję procesai (didėjantis interneto prieinamumas, technologijų tobulėjimas ir kt.) sudarė itin palankias sąlygas verslo subjektams panaudoti internete pasiekiamus asmens duomenis savo reikmėms. Europos Sąjungos Teisingumo Teismas pastebėjo, kad iš interneto vartotojų duomenų visumos gali būti daromos labai tikslios išvados apie asmenų privatų gyvenimą, kaip antai kasdienio gyvenimo įpročius, nuolatinę ar laikiną gyvenamąją vietą, kasdienį ir kitokį judėjimą, vykdomą veiklą, socialinius ryšius ir lankomą socialinę aplinką[3]. Toks duomenų pritaikomumas davė pradžią naujai reklamos internete rūšiai – būtent vartotojų elgsena grįstai reklamai. Iš vienos pusės, ši reklama padidina reikiamų vartotojų pasiekiamumą ir padeda parduoti daugiau produktų bei paslaugų. Tačiau, aplinkybė, kad vartotojų elgsena grįstos reklamos tikslais renkami ne bet kokie, o asmens duomenys, ir dažnai tokia veikla vykdoma nesilaikant aukščiau minėtų principų, sudaro įspūdį, jog asmenų privatus gyvenimas yra nuolat stebimas.

Europos Sąjungos atsakymas į susidariusias asmens duomenų rinkimo ir naudojimo problemas yra naujoji duomenų apsaugos reforma, atnešanti svarbius pokyčius iki šiol buvusiame teisiniame reguliavime. Tačiau, dar nepradėjus taikyti naujai priimtų teisės aktų nuostatų, jau keliami klausimai dėl jų veiksmingumo ir įgyvendinimo galimybių, o interneto vartotojai vis dažniau skatinami patys pasirūpinti savo duomenų apsauga[4]. Iš kitos pusės, viešojoje erdvėje kartkartėmis girdimą susirūpinimą seka kalbos apie vartotojų interesus atitinkančią reklamą, interneto vartotojų anonimiškumą, vartotojui draugiškas paslaugas ir pan. Tai skatina abejones dėl asmens duomenų rinkimo ir naudojimo internete problemų rimtumo, realumo. Vartotojų elgsena grįstos reklamos metodai paliečia kiekvieną interneto vartotoją be išimties, todėl išsiaiškinti potencialios grėsmės apimtį asmens duomenų saugumui ir privatumui yra itin svarbu.

---

[1] Europos Sąjungos pagrindinių teisių chartija. OL, 2012 C 326, p. 391.
[2] PETRAITYTĖ, I. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 165.
[3] Europos Sąjungos Teisingumo Teismas. 2014 m. balandžio 8 d. sprendimas *Digital Rights Ireland Ltd* C‑293/12 ir *Kärntner Landesregierung* C‑594/12, ECLI:EU:C:2014:238, 37 punktas.
[4] MATZNER, T., *et al. Do*-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 278.

Tyrimo objektas. Šiame darbe analizuojami elektroninėje erdvėje vykstančio asmens duomenų rinkimo ir naudojimo ryškiausi probleminiai aspektai Lietuvos ir Europos Sąjungos teisės kontekste. Darbe pasirinkta smulkiau analizuoti būtent asmens duomenų rinkimą ir naudojimą, kadangi, autoriaus vertinimu, šie veiksmai yra svarbiausi iš visų asmens duomenų tvarkymo elementų. Be asmens duomenų rinkimo ir naudojimo prasmės netenka kiti asmens duomenų tvarkymo veiksmai, t. y. nesant asmen duomenų surinkimui, nebus, ką įrašyti, saugoti, analizuoti ir pan. Taip pat, jeigu duomenys yra nenaudojami, nėra jokios prasmės juos rinkti, saugoti, gretinti ir pan. Asmens duomenis elektroninėje erdvėje įvairioms reikmėms renka ir naudoja tiek valstybės institucijos (pvz., žvalgyboje), tiek mokslo įstaigos (pvz., moksliniuose tyrimuose), tiek verslas. Darbe, nagrinėjant asmens duomenų rinkimo ir naudojimo problematiką, yra koncentruojamasi tik į verslo subjektų veiklą, o tiksliau, į jų veiklą, susijusia su internetine reklama. Reklama internete yra ypač aktuali šio darbo temai, kadangi tam tikrų jos rūšių[5], o būtent vartotojų elgsena grįstos reklamos, technologinis įgyvendinimas yra pagrįstas surinktų asmens duomenų panaudojimu.

Tyrimo tikslas. Išanalizavus asmens duomenų rinkimo ir naudojimo elektroninėje erdvėje teisinę aplinką bei technologines galimybes, atskleisti svarbiausias interneto vartotojų privatumui kylančias problemas, susijusias su vartotojų elgsena grįsta reklama, ir pasiūlyti galimus jų sprendimo būdus.

Atsižvelgiant į darbo tikslą, keliami tokie *uždaviniai:*

1. Atskleisti su asmens duomenimis elektroninėje erdvėje susijusio aktualaus teisinio reguliavimo ypatumus ir problemas;
2. Aptarti Europos Sąjungos asmens duomenų teisinės apsaugos reformos įtaką asmens privatumui elektroninėje erdvėje;
3. Išanalizuoti vartotojų elgsena grįstos reklamos veikimo principus ir technologinio įgyvendinimo metodus;
4. Ištirti asmens duomenų rinkimą ir naudojimą reglamentuojančių teisės normų įgyvendinimą subjektų, susijusių su vartotojų elgsena grįsta reklama, veikloje;
5. Nustatyti, kokia apimtimi už asmens duomenų apsaugą elektroninėje erdvėje turėtų būti atsakingas pats duomenų subjektas, priežiūros institucijos ir verslo subjektai.

[5] Pažymėtina, kad kitos internetinės reklamos rūšys darbe yra aptariamos tiek, kiek tai svarbu vartotojų elgsena grįstos reklamos turinio ir specifiškumo atskleidimui.

Darbo originalumas. Temos, susijusios su asmens duomenų teisinės apsaugos problemomis, Lietuvos moksliniuose darbuose nagrinėjamos gana retai[6]. Pažymėtina, kad dėl savo sudėtingumo ir plačios aprėpties, būtent elektroninės erdvės kontekste minėta tema dažniausiai nagrinėjama siauroje pasirinktoje srityje[7]. Atskirai paminėtinas išsamus ir šio darbo temai aktualus asmens duomenų bendrąją sampratą elektroninėje erdvėje analizuojantis Mindaugo Civilkos ir Linos Šlapimaitės straipsnis „Asmens duomenų samprata elektroninėje erdvėje“[8]. Iš šio darbo temai artimų magistro darbų paminėtini Dariaus Amšiejaus „Europos Sąjungos asmens duomenų apsaugos teisės reforma“[9] ir Aušros Činkaitės „Skaitmeninė reklama ir teisė į privatumą“[10]. Vis dėlto, skirtingai nuo minėtų magistro darbų, šiame darbe Europos Sąjungos asmens duomenų reforma aptariama būtent elektroninės erdvės požiūriu, o skaitmeninė reklama analizuojama asmens duomenų rinkimo bei naudojimo kontekste ir tik tiek, kiek ji susijusi su vartotojų elgsena grįsta reklama ir jos metodais.

ES įvairių mokslinių straipsnių asmens duomenų apsaugos, privatumo elektroninėje erdvėje klausimais vis daugėja, ypač po Europos Sąjungos asmens duomenų reformos pradžios. Vis dar pasigendama didesnės apimties mokslinių darbų (pavyzdžiui, monografijų) šia tema, tačiau, pagal viešojoje erdvėje pateiktą informaciją, nemažai aktualių temai knygų turėtų pasirodyti dar iki 2017 metų pabaigos[11].

Tyrimo šaltiniai. Šio darbo pagrindą sudaro Lietuvos ir Europos Sąjungos asmens duomenų apsaugos srityje taikomi teisės aktai, kompetentingų institucijų rekomendacijos ir nuomonės, taip pat teisės ir kitų sričių mokslinė literatūra. Svarbiausi analizuojami teisės aktai darbe – tai Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas, Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos

[6] Paminėtini: PETRAITYTĖ, I. Asmens duomenų teisinės apsaugos principai: daktaro disertacija. Vilnius, 2013, taip pat tos pačios autorės straipsniai PETRAITYTĖ, I. Asmens duomenų apsaugos teisinis reguliavimas Lietuvos teisės sistemoje. *Teisė*, 2011, t. 79, p. 125-138 ir PETRAITYTĖ, I. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174. Be to, paminėtinas Dalios Misiūnaitės-Kamarauskienės straipsnis Europos Sąjungos Teisingumo Teismo praktikos aktualijos pagrindinių teisių į privatų ir šeimos gyvenimą bei asmens duomenų apsaugą srityje. *Jurisprudencija*, 2014, t. 21(4), p. 1233-1245.

[7] Tokie pavyzdžiai galėtų būti DAUPARAITĖ, I., *et al*. *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011. Taip pat Viktorijos Bessonovos magistro darbas Asmens duomenų debesų kompiuterijoje teisinė apsauga. Vilnius, Vilniaus universitetas, 2013.

[8] CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126-148;

[9] AMŠIEJUS, D. Europos Sąjungos asmens duomenų apsaugos teisės reforma: magistro darbas. Vilnius, Vilniaus universitetas, 2014.

[10] ČINKAITĖ, A. Skaitmeninė reklama ir teisė į privatumą: magistro darbas. Vilnius, Vilniaus universitetas, 2015.

[11] Kai kurių užsienio autorių knygos asmens duomenų teisinės apsaugos elektroninėje erdvėje temomis turėtų pasirodyti dar iki 2017 metų pabaigos, pavyzdžiui KELLEHER, D., MURRAY, K. EU Data protection Law. London: Bloomsbury Publishing PLC, 2017; PSYCHOGIOPOULOU, E. Courts, privacy and data protection in the digital environment. Cheltenham: Edward Elgar Publishing Ltd, 2017 ir kt.

tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo bei Europos Parlamento ir Tarybos reglamentas 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). Iš teisės srities mokslinių straipsnių verta išskirti *S. Gutwirth* kartu su kitais autoriais sudarytus straipsnių rinkinius[12], kuriuose itin įdomiai ir išsamiai nagrinėjamos su asmens duomenų tvarkymu internete susijusios problemos.

Tyrimo metodai. Darbe naudojami teleologiniu, lyginamuoju bei loginiu analitiniu metodais. Teleologiniu metodu siekiama nustatyti analizuojamų teisės normų tikruosius tikslus. Pavyzdžiui, darbe bandoma nustatyti Europos Sąjungos duomenų apsaugos reformą sąlygojusias priežastis ir ja siekiamus tikslus. Lyginamuoju metodu daugiausia remtasi gretinant teisinį reguliavimą Lietuvoje ir Europos Sąjungoje, taip pat šiuo metu taikomus teisės aktus ir Bendrąjį duomenų apsaugos reglamentą. Šiuo metodu norėta atskleisti teisinio reguliavimo vystymąsi ir jo rezultatus. Loginiu analitiniu metodu naudojamasi siekiant pateikti teisinio reguliavimo ir vartotojų elgsena grįstos reklamos metodų vertinimą bei suformuojant galutines išvadas. Darbo eigoje taip pat atliktas empirinis tyrimas, kurio metu buvo siekiama ištirti asmens duomenų rinkimą ir naudojimą reglamentuojančių teisės normų įgyvendinimo laipsnį tam tikrų Lietuvos verslo subjektų (o būtent – jų valdomų interneto tinklalapių) veikloje.

Darbo struktūra. Atsižvelgiant į darbo objektą, tikslą ir išsikeltus uždavinius, darbo struktūra susideda iš įžangos, keturių dėstomųjų dalių (atskirai skirstomų į skyrius), darbo išvadų ir literatūros sąrašo. Pirmojoje dalyje analizuojama galiojančiame teisiniame reglamentavime įtvirtinta asmens duomenų samprata, asmens duomenų tvarkymo elektroninėje erdvėje ypatybės bei taikytinos teisės problemos. Antroje darbo dalyje nagrinėjamas Bendrajame duomenų apsaugos reglamente įtvirtintos temai aktualios teisinio reguliavimo naujovės. Darbo trečioje dalyje atskleidžiami vartotojų elgsena grįstos reklamos samprata ir metodai bei aptariamos su teisės reikalavimų toje srityje įgyvendinimu susijusios problemos. Ketvirtoje dalyje stengiamasi nustatyti duomenų subjekto, priežiūros institucijų ir verslo subjektų atsakomybės asmens duomenų apsaugos srityje ribas.

[12] GUTWIRTH, S., *et al. Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Law, Governance and Technology, vol. 24. Belgium: Springer, 2016. Taip pat GUTWIRTH, S., *et al. Reforming European Data Protection Law*. Law, Governance and Technology, vol. 20. Belgium: Springer, 2015.

1. ASMENS DUOMENŲ ELEKTRONINĖJE ERDVĖJE TEISINIO REGULIAVIMO YPATUMAI

1.1 Asmens duomenų samprata

Lyginant asmens duomenų sampratą, įtvirtintą Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo[13] (toliau – ADTAĮ) įsigaliojimo pradžioje, t. y. 1996 metais, ir šiuo metu galiojančioje redakcijoje[14], galima netiesiogiai stebėti ir tam tikrą Lietuvos visuomenės raidą, susijusią ne tik su įstojimu į Europos Sąjungą (toliau ir – ES), bet ir su kompiuterinių technologijų modernėjimu ir palaipsniu įvairios veiklos perkėlimu į elektroninę erdvę. Pirmoji ADTAĮ redakcija, teturinti tik 14 straipsnių, buvo skirta santykių tarp fizinių ar juridinių asmenų bei valstybės kompiuterizuotų informacinių sistemų valdytojų sureguliavimui. Asmens duomenimis buvo laikoma tik siaura informacijos apie asmenį dalis – duomenys apie konkretų arba iš duomenų nustatomą fizinį asmenį, jo dalykinius santykius ir išvados apie asmenį, padarytos remiantis šiais duomenimis[15]. Vis dėlto, supratus, kad plintant technologijoms asmens duomenis dažnai tvarko ne vien valstybės įgalioti asmenys ir institucijos, o kartu asmens duomenys neapsiriboja vien asmens kodu, vardu, pavarde ir pan., buvo praplėsta įstatymo apsaugos sritis ir jai priskirta beveik visa asmens informacija, tvarkoma automatiniu ar neautomatiniu būdu, ir ne vien valstybės. Taigi, teisinis reguliavimas ADTAĮ buvo suderintas su reguliavimu, nustatytu 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyvoje 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo[16] (toliau – 95/46/EB direktyva).

Vadovaujantis ADTAĮ 2 str. 1 d., asmens duomenimis laikoma bet kuri informacija, susijusi su fiziniu asmeniu – duomenų subjektu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta pasinaudojant tokiais duomenimis kaip asmens kodas, vienas arba keli asmeniui būdingi fizinio, fiziologinio, psichologinio, ekonominio, kultūrinio ar socialinio pobūdžio požymiai. Ši sąvoka yra iš esmės identiška nustatytajai 95/46/EB direktyvoje ir yra sudaryta iš trijų pagrindinių elementų: 1) bet kurios informacijos; 2) informacijos sąsajumo su fiziniu asmeniu; 3) asmens tapatybės

[13] Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, Nr. 63-1479.
[14] t. y. ADTAĮ redakcijoje, galiojančioje nuo 2017 m. sausio 1 d.
[15] žr. ADTAĮ 2 str. 1 d., galiojusią redakcijose nuo 1996 m. liepos 3 d. iki 2001 m. sausio 1 d.
[16] 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL, 1995 L 281, p. 31.

nustatymo ar galimybės ją nustatyti[17]. Toliau tekste pateikiama detalesnė minėtų elementų analizė.

1) Pirmiausia, informacija tiek 95/46/EB direktyvoje, tiek ADTAĮ suprantama labai plačiai: jai nekeliami objektyvumo, teisingumo reikalavimai, nekreipiamas dėmesys į formatą (asmens duomenys gali būti pateikti vaizdinėje, rašytinėje, garsinėje ar bet kokioje kitoje formoje), netgi turinio prasme asmens duomenimis bus pripažinta ir informacija, talpinanti ypatinguosius asmens duomenis[18], ir bendresnio pobūdžio informacija, taip pat tiek informacija susijusi su asmeniniu ar šeimos gyvenimu, tiek informacija apie asmens vykdomą veiklą, ekonominį, socialinį elgesį[19]. Atkreiptinas dėmesys, kad į asmens duomenų sąvoką taip pat patenka biometriniai duomenys (t. y. pirštų antspaudai, balsas, rainelės struktūra, įgūdis ar tam tikra elgesio ypatybė)[20].
2) Antra, asmens duomenys turi talpinti informaciją, kuri yra susijusi su fiziniu asmeniu ją vertinant pagal bent vieną iš šių elementų: turinio, tikslo arba rezultato[21]. Informacija yra susijusi su asmeniu pagal turinį, kai ji yra apie tą konkretų asmenį, pavyzdžiui, tai to asmens nuotrauka, asmens kodas, asmens pažymių knygelė. Informacija yra sąsaji pagal tikslą, kai atsižvelgiant į konkrečias aplinkybes duomenys naudojami siekiant įvertinti asmens padėtį, nagrinėti elgesį ar daryti tam įtaką, pavyzdžiui, patalpos signalizacijos įjungimo ir išjungimo registravimas, siekiant nustatyti, kada asmuo atėjo ar išėjo iš patalpos. Sąsajumas pagal rezultatą lemia, kad naudojimasis šiais duomenimis gali daryti (net ir nedidelį) poveikį konkretaus asmens teisėms ir interesams, pavyzdžiui, surinkta informacija gali lemti, jog asmuo įgis liudytojo statusą[22]. Atkreiptinas dėmesys, kad 95/46/EB direktyvoje ir ADTAĮ reglamentuojama asmens duomenų apsauga taikoma visiems fiziniams asmenims, neapsiribojant pilietybe ar gyvenamąja vieta. Informacijai apie juridinius asmenis šių teisės aktų apsauga gali būti taikoma nebent tuo atveju, jei tokia informacija yra iš esmės susijusi su fiziniais asmenimis pagal aukščiau aprašytus turinio, tikslo ar rezultato elementus.

[17] 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. priimta „Nuomonė 4/2007 dėl asmens duomenų sąvokos“, 01248/07/LT, WP136, p. 5.
[18] Ypatingais duomenimis vadinami duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą (žr. ADTAĮ 2 str. 8 d., analogiškai ir 95/46/EB direktyvos 8 str.).
[19] 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. priimta „Nuomonė 4/2007 dėl asmens duomenų sąvokos“, 01248/07/LT, WP136, p. 6-8.
[20] *Ibid.*
[21] *Ibid.*, p. 10.
[22] CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. Teisė, 2015, t. 96, p. 134.

3) Trečia, pagal duomenis, atitinkančius asmens duomenų sąvoką, turi būti įmanoma išskirti asmenį iš tam tikros asmenų grupės, nustatyti jo tapatybę. Asmens tapatybę gali sudaryti bet koks vardas, numeris ar kitas požymis, kuris suteikia informacijos apie asmenį ar kuriuo pasinaudojus galima prieiti prie kitų asmens duomenų[23]. Atitinkamai, ji gali būti nustatoma tiesiogiai, t. y. pagal nuorodą į vardą ir pavardę. Šiuo atveju asmens vardas ir pavardė dažnai susiejamas ir su papildoma informacija (pavyzdžiui, gimimo diena, adresu, nuotrauka ir pan.), siekiant asmenį identifikuoti tiksliau. Tapatybė gali būti nustatoma ir netiesiogiai, kai pirminiai duomenys dar neleidžia išskirti konkretaus asmens, tačiau sudėjus tuos duomenis su kita informacija (kurių duomenų valdytojas gali dar net neturėti[24]) yra ar gali būti įmanoma išskirti asmenį iš tam tikros grupės. Pažymėtina, kad identifikuojant asmens duomenis reikia įvertinti realią galimybę išskirti asmenį iš grupės. Tai reiškia būtinybę atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar kuris kitas asmuo. Jeigu tokių priemonių nėra ar galimybės jomis pasinaudoti yra nedidelės, informacija neturėtų būti laikoma asmens duomenimis[25].

Visi šie tarpusavyje glaudžiai susiję elementai asmens duomenis nuo bet kokios kitos informacijos turėtų padėti atskirti tiek fizinėje[26], tiek elektroninėje erdvėje. Šios dvi erdvės reikšmingai skiriasi viena nuo kitos, todėl kyla klausimas, ar minėtieji elementai pakankamai tiksliai apibūdina asmens duomenis skirtinguose kontekstuose. Į šį klausimą galima atsakyti tik tinkamai išanalizavus fizinės ir elektroninės erdvės skirtumus.

1.2 Asmens duomenų elektroninėje erdvėje ypatumai

Teisinėje literatūroje elektroninė erdvė apibūdinama kaip „nepriklausoma, neturinti fizinių ir teisinių sienų komunikacijos aplinka, neturinti centralizuoto valdymo ar

[23] DAUPARAITĖ, I., *et al. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011, p. 18.

[24] Europos Sąjungos Teisingumo Teismas yra pasisakęs, jog tam, kad informacija būtų laikoma asmens duomenimis, nebūtina, kad ji pati savaime leistų nustatyti atitinkamo asmens tapatybę. Norint įvertinti, ar asmens tapatybė gali būti nustatyta, reikėtų atsižvelgti į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo minėto asmens tapatybei nustatyti. Nėra reikalaujama, kad visą informaciją, leidžiančią nustatyti atitinkamo asmens tapatybę, turėtų vienas asmuo (Europos Sąjungos Teisingumo Teismas. 2016 m. spalio 19 d. sprendimas *Patrick Breyer / Bundesrepublik Deutschland* C‑582/14, ECLI:EU:C:2016:779, 40-44 punktai).

[25] 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. priimta „Nuomonė 4/2007 dėl asmens duomenų sąvokos“, 01248/07/LT, WP136, p. 6-8.

[26] Fizinė erdvė šiame darbe suprantama kaip visuomeninių santykių, susiklosčiusių ne elektroninėje erdvėje, vieta.

centralizuotų kontrolės mechanizmų“[27]. Internetas yra vienas iš elektroninės erdvės elementų, tačiau praktikoje šios dvi sąvokos yra dažnai naudojamos kaip sinonimai. Šiame darbe sąvokos internetas ir elektroninė erdvė taip pat bus suprantamos kaip turinčios tą pačią reikšmę. Turint omenyje, kad elektroninės ir fizinės erdvės skirtybės šiame darbe yra aktualios tiek, kiek jos susijusios su asmens duomenų tema, yra tikslinga esminius skirtumus tarp fizinės ir elektroninės erdvės aptarti atsižvelgus į aukščiau nagrinėtus asmens duomenų sampratos pagrindinius elementus.

1) *Informacija*. Tiek fizinėje, tiek elektroninėje erdvėje informacija, turinti potencialo tapti asmens duomenimis, suprantama labai plačiai. Šiuo aspektu minėtos erdvės viena nuo kitos nesiskiria, tačiau atkreiptinas dėmesys, kad tiek fizinės, tiek elektroninės erdvės sąveikavimas tarpusavyje praplečia informacijos, kuri galėtų būti laikoma asmens duomenimis, apimtį. Pavyzdžiui, kompiuterio IP adresas[28] arba asmens elektroninis parašas yra išimtinai elektroninės erdvės komponentas, tačiau IP adreso ar elektroninio parašo kodą perkėlus į fizinę erdvę (pavyzdžiui, atspausdinus ant popieriaus lapo) ši informacija, atsižvelgiant į kitas sąlygas, galėtų būti laikoma asmens duomenimis ir fizinėje erdvėje.
2) *Sąsajumas*. Analogiškai, informacijos sąsajumas su fiziniu asmeniu pagal turinį, tikslą ar rezultatą gali būti nustatomas tiek elektroninėje, tiek fizinėje erdvėje. Teisės doktrinoje tik atkreipiamas dėmesys, kad, skirtingai nei fizinėje erdvėje, kur asmeninė informacija visos informacijos kontekste laikoma išimtimi, elektroninėje erdvėje išimtimi tampa informacija, neturinti jokio ryšio su asmeniu[29]. Elektroninėje erdvėje informacijos sąsajumas su asmeniu iš tiesų pasireiškia žymiai dažniau ir įvairesnėmis formomis, kadangi, naršydamas elektroninėje erdvėje, asmuo beveik visada palieka savo elgesio pėdsakus (pavyzdžiui, aplankyta internetinė svetainė užfiksuoja apsilankymo laiką, asmens paspaustas nuorodas, jo IP adresą).
3) *Asmens tapatybės nustatymas*. Didžiausi skirtumai tarp elektroninės ir fizinės erdvės atsiskleidžia nagrinėjant asmens tapatybės nustatymo (identifikavimo galimybės) klausimus. Teisinėje literatūroje nurodoma, kad paprastai fizinėje erdvėje asmuo išskiriamas iš kitų asmenų tarpo, kai pateikia tinkamą asmens dokumentą, išduotą valstybės institucijų (pavyzdžiui, gimimo liudijimas, asmens tapatybės kortelė ar kt.)

[27] DAUPARAITĖ, I., *et al. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011, p. 34.
[28] Sąvoka „IP adresas“ šiame darbe vartojama kaip interneto protokolo adreso trumpinys.
[29] CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. Teisė, 2015, t. 96, p. 136.

ar kitų subjektų (pavyzdžiui, darbdavio išduotas darbuotojo pažymėjimas)[30]. Manytina, kad identifikavimas fizinėje erdvėje neapsiriboja tik tiesioginiu asmens tapatybės nustatymu iš pateikto dokumento. Minėta, jog asmuo gali būti identifikuojamas ir netiesiogiai, o tokie atvejai būdingi ir fizinei erdvei (pavyzdžiui, nusikaltęs asmuo gali būti atpažįstamas pagal jo pirštų antspaudus, paliktus nusikaltimo vietoje). Galima spręsti, kad asmens identifikavimas fizinėje erdvėje nėra labai dažnas reiškinys paprasčiausiai dėl to, jog daugumoje kasdienių situacijų asmens tapatybės nustatymas nėra būtinas. Pavyzdžiui, asmeniui apsiperkant parduotuvėje fizinėje erdvėje, paprastai nėra būtina identifikuoti konkretų žmogų, tačiau apsiperkant internetu, asmuo turi pateikti duomenis (pavyzdžiui, vardą, pavardę, adresą ir pan.), kurie leistų išskirti asmenį iš kitų vien jau tam, kad pirkinys būtų tinkamai pristatytas. Taigi, elektroninėje erdvėje dėl šios erdvės specifikos (t. y. asmuo konkrečiame santykyje tiesiogiai nedalyvauja) asmens identifikavimas vyksta dažniau nei fizinėje erdvėje. Tačiau tai tikrai nėra vienintelis elektroninės erdvės išskirtinumas šiuo aspektu. Asmuo elektroninėje erdvėje gali būti identifikuojamas daug daugiau būdų nei fizinėje erdvėje, t. y. ne tik savanoriškai pateikdamas savo specifinius duomenis trečiajam asmeniui. Elektroninėje erdvėje veikiančios technologijos sudaro galimybę apjungti įvairius ten jau egzistuojančius duomenis (angl. *to aggregate*) bei apjungimo rezultatą panaudoti asmenų identifikavimui. Dar daugiau, internete egzistuojantis didžiulis prieinamumas prie įvairios su asmeniu susijusios informacijos duomenų apjungimą padaro lengviau įgyvendinamu[31]. Fizinėje erdvėje toks spartus ir tikslus duomenų apjungimas būtų neįmanomas. Elektroninėje erdvėje egzistuojanti įvairios informacijos apjungimo galimybė dažnai panaikina ribas tarp asmenį identifikuojančių ir neidentifikuojančių duomenų. Kitaip tariant, internete kiekviena su asmeniu susijusi informacija gali potencialiai identifikuoti tą asmenį, o, ar asmuo bus tikrai identifikuotas, priklauso tik nuo išteklių ir pastangų, kurias konkrečiu atveju norima skirti[32]. Teisės literatūroje yra pateikiama pavyzdžių, kai tam tikri duomenys, kurie paimti atskirai, negali būti susieti su konkrečiu asmeniu, juos apjungiant, gali tą asmenį identifikuoti. Pavyzdžiui, JAV atliktų tyrimų rezultatai parodo, kad duomenų kombinacija, susidedanti vien iš pašto kodo, gimimo datos ir

[30] DAUPARAITĖ, I., *et al. Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011, p. 21.
[31] SCHWARTZ, P. M., SOLVE, D. J. The PII problem: privacy and a new concept of personally identifiable information. New York university law review, 2011 December, Vol. 86:1814, p. 1842.
[32] CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. Teisė, 2015, t. 96, p. 137.

lyties, yra pakankama nustatyti 87% JAV gyvenančių asmenų[33]. Atskiri duomenys, tokie kaip pašto kodas, negali būti laikomi asmenį identifikuojančiais, kadangi tuo pačiu pašto kodu naudojasi daug konkrečioje vietoje gyvenančių žmonių, tačiau, apjungus šį duomenį su kitais nurodytais, jų visuma sudaro galimybę asmens identifikavimui. Pažymėtina, kad tokiam duomenų apjungimui internete dažnai nėra būtini dideli ištekliai ar itin specifinės žinios. Turima informacija įvairių paieškos sistemų pagalba tiesiog gretinama su internete (pavyzdžiui, socialiniuose tinkluose ar duomenų bazėse) esančia informacija, kol aptinkami tam tikri tarpusavio ryšiai, kurie leidžia išskirti asmenį ar kelis asmenis iš grupės. Taigi, asmens identifikavimo galimybėmis elektroninė erdvė smarkiai pranoksta fizinę erdvę.

Atsižvelgus į čia aptartą fizinės ir elektroninės erdvės specifiką, darytina išvada, kad Europos Sąjungoje, o kartu ir Lietuvoje, pripažįstama asmens duomenų samprata yra pakankamai pažangi. Kaip jau minėta, asmens duomenimis laikomi tokie duomenys, kurie ne tik identifikuoja konkretų asmenį realiu laiku, bet ir tokie, kurie sudaro galimybę asmenį identifikuoti juos apjungus su kita informacija[34]. Vis dėlto, toks išplėstinis požiūris Europos Sąjungoje sulaukia ir kritikos tuo aspektu, kad tiek asmenį identifikuojanti, tiek potencialiai identifikuojanti informacija yra traktuojama vienodai, t. y. jai taikomi tie patys reikalavimai ir toks pat apsaugos lygis[35]. Pavyzdžiui, 95/46/EB direktyvos 12 straipsnyje yra įtvirtinta taisyklė, kad, duomenų subjektui pareikalavus, duomenų valdytojas, be kita ko, turi pateikti pranešimą suprantamu pavidalu apie tvarkomus duomenis ir bet kurią prieinamą informaciją apie jų šaltinius (panašų reguliavimą nustato ir ADTAĮ 25 str.). Toks reikalavimas gali būti suprantamas, kai kalbama apie duomenis, kurie jau identifikuoja asmenį. Tačiau tikras nesusipratimas to reikalauti iš duomenų valdytojo, turinčio tik asmenį potencialiai identifikuojančią informaciją, kadangi, norint įsitikinti, ar informacija susijusi su jos prašančiu duomenų subjektu, duomenų valdytojui tektų pirma visą turimą informaciją susieti su tuo konkrečiu duomenų subjektu. Taigi, duomenų valdytojui tektų naudoti papildomus išteklius vien tam, kad tą informaciją pateiktų, o kartu, susiejęs duomenis su konkrečiu asmeniu, jis savo dispozicijoje jau turėtų nebe potencialiai, o realiai asmenį identifikuojančią

[33] SWEENEY, L. *Simple Demographics Often Identify People Uniquely*. Data Privacy Working Paper 3. Pittsburgh: Carnegie Mellon University, 2000, p. 16.
[34] Palyginimui, JAV laikosi pozicijos, kad informacija, kuri tik sudaro galimybę asmenį identifikuoti, bet jo realiai neidentifikuoja (angl. *personal identifiable information*), nėra savaime laikytina asmens duomenimis (Žr. SCHWARTZ, P. M., SOLVE, D. J. The PII problem: privacy and a new concept of personally identifiable information. New York university law review, 2011 December, Vol. 86:1814, p. 1871).
[35] SCHWARTZ, P. M., SOLVE, D. J. The PII problem: privacy and a new concept of personally identifiable information. New York university law review, 2011 December, Vol. 86:1814, p. 1872.

informaciją, kurios jam galbūt net nereikėjo. Šiuo atveju kritikuojama turėtų būti ir duomenų subjekto teisė reikalauti turimus duomenis ištaisyti, patikslinti.

Turint omenyje šias problemas, vis dažniau pasigirsta siūlymų asmenį identifikuojančius ir potencialiai identifikuojančius duomenis traktuoti skirtingai[36]. Pavyzdžiui, pastariesiems taikyti švelnesnį režimą, kuriam galbūt užtektų tik pateikti informaciją apie daromą poveikį duomenų subjektų grupei. Tačiau, prieš susikoncentruojant į galimas asmens duomenų tvarkymo teisinio reguliavimo kryptis, būtina įdėmiau apžvelgti dabartines duomenų tvarkymo ypatybes, o tai bus padaryta kitoje darbo dalyje.

1.3 Asmens duomenų tvarkymo elektroninėje erdvėje specifika

Tiek 95/46/EB direktyvoje, tiek ADTAĮ įtvirtinta duomenų tvarkymo samprata iš esmės reiškia, kad kone visiems veiksmams, atliktiems su asmens duomenimis, bus taikomi tam tikri specifiniai reikalavimai. Asmens duomenų tvarkymas yra apibūdinamas kaip bet kuris su asmens duomenimis atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas (papildymas ar taisymas), teikimas, paskelbimas, naudojimas, loginės ir (arba) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų rinkinys (ADTAĮ 2 str. 4 d.). Pažymėtina, kad, jei su asmens duomenimis yra atliekamas daugiau nei vienas veiksmas, tai duomenų tvarkymu bus laikoma visa tų veiksmų procedūra, atliekant konkrečią užduotį[37]. Į šią sąvoką patenka duomenų tvarkymas tiek automatiniu[38], tiek neautomatiniu[39] būdu, ir abiems būdams yra taikomas vienodas teisinis reguliavimas.

Pagrindinis asmens duomenų teisinės apsaugos elementas yra tikslingumas ir būtent asmens duomenų tvarkymo tikslingumas apibrėžia, ar toks duomenų tvarkymas yra teisėtas[40]. Taigi, prieš pradėdamas tvarkyti asmens duomenis, duomenų valdytojas turi aiškiai ir vienareikšmiškai apsibrėžti savo teisėtus tikslus (juos identifikuoti turi gebėti tiek duomenų subjektas, tiek priežiūros institucija), ir po to privalo tvarkyti duomenis tuos

[36] CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. Teisė, 2015, t. 96, p. 141.
[37] Asmens duomenų teisinės apsaugos įstatymo komentaras. Vilnius, 2005, p. 14.
[38] Duomenų tvarkymas automatiniu būdu – duomenų tvarkymo veiksmai, visiškai ar iš dalies atliekami automatinėmis priemonėmis (ADTAĮ 2 str. 5 d.). Pažymėtina, jog jeigu dalis veiksmų bus atliekama automatinėmis, o dalis neautomatinėmis priemonėmis, bus laikoma, kad duomenų tvarkymas vis tiek vykdomas automatiniu būdu.
[39] Duomenų tvarkymas neautomatiniu būdu – veiksmai, atliekami tvarkant asmens duomenų susistemintas rinkmenas (ADTAĮ 1 str. 2 d.).
[40] JENTS, L., KELLI, A. Legal aspects of processing personal data in development and use of digital language resources: the Estonian perspective. *Jurisprudencija*, 2014, 21(1), p. 171.

tikslus atitinkančiais būdais[41]. Atsižvelgiant į suformuotus tikslus, duomenų tvarkymui yra taikomi ADTAĮ 3 straipsnyje (95/46/EB direktyvos 6 str. 1 dalyje) nustatyti principai: duomenų tikslumas, naujumas, išsamumas, pobūdžio ir apimties proporcingumas, minimaliai trumpa asmens duomenų saugojimo trukmė. Minėti teisės aktai (būtent ADTAĮ 5 str. ir 95/46/EB direktyvos 7 str.) taip pat nustato duomenų tvarkymo kriterijus, kurie apsprendžia, kada apskritai asmens duomenys gali būti tvarkomi. Šie kriterijai apima atvejus, kai duomenų subjektas duoda sutikimą, su duomenų subjektu tuo klausimu sudaroma ar vykdoma sutartis, duomenų valdytojas yra įstatymiškai įpareigotas tvarkyti asmens duomenis, yra siekiama apsaugoti duomenų subjekto esminius interesus, įgyvendinami oficialūs institucijų įgaliojimai arba duomenis reikia tvarkyti dėl teisėto intereso, kurio siekia duomenų valdytojas arba trečiasis asmuo, ir jei duomenų subjekto interesai nėra svarbesni.

Šio darbo kontekste autorių labiausiai domina du iš paminėtų asmens duomenų tvarkymo kriterijų – tai duomenų subjekto duotas sutikimas ir teisėti duomenų valdytojo ar trečiojo asmens interesai. Darbe siekiama apžvelgti ne išimtinius asmens duomenų tvarkymo atvejus, susijusius su tam tikrais įgaliojimais (įstatymų įpareigotas tvarkymas, tvarkymas, atliekamas saugant esminius interesus ar vykdant įgaliojimus), ir ne atvejus, kai paties duomenų subjekto tikslas yra jo asmens duomenų tvarkymas (sutarties vykdymo atvejai). Toliau aptariami kriterijai yra artimiausi elektroninėje erdvėje vykdomam standartinio interneto vartotojo duomenų tvarkymui, su kuriais jis galimai susiduria kas kartą atsidūręs elektroninėje erdvėje. Toliau taip pat bus atskirai apžvelgti ypatingųjų asmens duomenų tvarkymo reikalavimai.

1. *Duomenų tvarkymas iš duomenų subjekto gauto sutikimo pagrindu*

Duomenų subjekto duotas sutikimas yra pirmasis ir svarbiausias iš išvardintų šešių duomenų tvarkymo kriterijų. Jis suteikia duomenų subjektui galimybę pasisakyti dėl savo duomenų tvarkymo. Tačiau sutikimo gavimas jokiu būdu nereiškia, kad nereikia laikytis kitų duomenų apsaugos principų, o kartu jis nepanaikina būtinybės tokiam duomenų tvarkymui taikyti ADTAĮ 3 straipsnyje nurodytus reikalavimus (pavyzdžiui, duomenų

[41] Duomenų tvarkymo tikslingumo svarba akcentuojama ir Lietuvos teismų praktikoje. Pasak Lietuvos Aukščiausiojo Teismo, ADTAĮ 3 str. 1 d. 1 p. nustatyto pareigą duomenų valdytojui užtikrinti, kad asmens duomenys būtų renkami apibrėžtais ir teisėtais tikslais ir toliau nebūtų tvarkomi tikslais, nesuderinamais su nustatytaisiais prieš renkant asmens duomenis, o to paties straipsnio 1 dalies 2 punktas įtvirtina pareigą asmens duomenis tvarkyti tiksliai, sąžiningai ir teisėtai (žr., pavyzdžiui, Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. birželio 17 d. nutartis administracinio teisės pažeidimo byloje Valstybinė duomenų apsaugos inspekcija v. R. S. Nr. 2AT-59-976/2015*).

subjekto sutikimas nekompensuoja imperatyvaus tikslingumo principo nesilaikymo[42]). Duomenų subjekto suteiktas sutikimas taip pat gali būti naudojamas kartu su kitais kriterijais (pavyzdžiui, kaip papildoma sąlyga, norint viršyti sutartyje su duomenų subjektu aptartą tvarkomų duomenų apimtį). Duomenų subjekto duotam sutikimui nėra svarbu jo išreiškimo forma (galima sutikti raštu, žodžiu ar net konkliudentiniais veiksmais), tačiau yra taikomas nedviprasmiškumo reikalavimas[43]. Taigi, kai duomenų subjektas išreiškia savo sutikimą, šis veiksmas neturi palikti vietos abejonėms, susijusioms su jo ketinimu (ypač tai aktualu siekiant gauti duomenų subjekto sutikimą elektroninėje erdvėje). Nedviprasmišku sutikimu nebus laikomos asmenų tylėjimu ar neveikimu grindžiamos sutikimo gavimo procedūros, kadangi asmens tylėjimui ar neveikimui yra savaime būdingas dviprasmiškumas (tai gali reikšti, kad duomenų subjektas nori sutikti, bet gali reikšti ir tai, kad jis tiesiog neatliko veiksmo)[44]. Pavyzdžiui, tais atvejais, kai asmenims yra pranešama, jog jų neatsakymas į pranešimą bus suprastas kaip sutikimas leisti tvarkyti asmens duomenis, asmens neveikimas kelia abejonių dėl jo noro išreikšti sutikimą. Todėl pasyvumas negali reikšti, jog duomenų subjektas duoda sutikimą savo duomenų tvarkymui, nes tai neatitinka nedviprasmiškumo reikalavimo. Dėl tokio reikalavimo duomenų valdytojai, siekdami gauti asmenų sutikimus, yra priversti sukurti aiškią tvarką, kuri leistų prašyti neabejotino sutikimo arba kuri sudarytų sąlygas aiškiam numanomam sutikimui gauti. Be to, duomenų valdytojas turi būti tikras, kad sutikimą duodantis asmuo iš tiesų yra duomenų subjektas[45]. Beje, sutikimą gavęs duomenų valdytojas turi sugebėti įrodyti sutikimo gavimo faktą, pavyzdžiui, to pareikalavus priežiūros institucijai ar kilus ginčui su duomenų subjektu. Tai dar vienas argumentas, kodėl neturėtų būti pasikliaujama duomenų subjekto neveikimu ir iš to preziumuojama, jog sutikimas duotas, kadangi reikiamu atveju gali būti sunku įrodyti, kad asmuo iš tiesų dėl to sutiko[46]. Tam, kad duomenų subjekto duotas sutikimas būtų tinkamas, jis turi būti ne tik nedviprasmiškas, bet ir duotas savanoriškai, konkretus ir pagrįstas informacija. Tai reiškia, kad prieš duomenų subjektą negali būti naudojama apgaulė, jis neturi būti bauginamas kokiais nors jam neigiamais padariniais. Kartu, prieš duomenų subjektui išreiškiant sutikimą, jam turi būti suteikiama suprantama (ne pernelyg

[42] Valstybinės duomenų apsaugos inspekcija. Rekomendacijos duomenų valdytojams dėl asmens duomenų tvarkymo etikos kodeksų rengimo, 2005, p. 2.
[43] Nedviprasmiškai duotas duomenų subjekto sutikimo reikalavimas yra *expressis verbis* pateiktas 95/46/EB direktyvos 7 straipsnyje. Atkreiptinas dėmesys, jog tokio įvardijimo nėra ADTAĮ 5 straipsnyje, tačiau atsižvelgiant į ADTAĮ 2 str. 12 p. formuluotę bei tai, kad ADTAĮ yra suderinta su 95/46/EB direktyvos nuostatomis, manytina, jog toks reikalavimas yra taikomas ir ADTAĮ.
[44] 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. priimta „Nuomonė 4/2007 dėl asmens duomenų sąvokos“, 01248/07/LT, WP136, p. 23.
[45] *Ibid.,* p. 20.
[46] *Ibid.,* p. 21.

sudėtingu teisiniu ar techniniu žodynu pagrįsta), aiški (ne bendro pobūdžio) ir akivaizdi (lengvai pastebima) informacija, kuri užtikrintų, kad sutikimas buvo duotas duomenų subjektui suprantant, su kuo jis sutinka[47]. Taigi, visoms šioms sąlygoms esant, asmens duomenų tvarkymas, gavus duomenų subjekto sutikimą, bus laikomas teisėtu.

2. *Duomenų tvarkymas dėl teisėto intereso, kurio siekia duomenų valdytojas*

Kalbant apie asmens duomenų tvarkymą, kai tvarkoma dėl teisėto intereso, kurio siekia duomenų valdytojas arba trečiasis asmuo, reikia pažymėti, kad tai yra vienintelis duomenų tvarkymo kriterijus, kurio teisėtumas, jau egzistuojant visoms būtinoms sąlygoms, papildomai vertinamas atsižvelgiant į konkrečią situaciją. Tai yra, šiuo atveju atliekamas interesų subalansavimo testas, kuris įvertina teisėtus duomenų valdytojo ar trečiojo asmens interesus ir juos pasveria prieš duomenų subjekto interesus, turimas fundamentalias teises ir laisves. Šio testo rezultatas apsprendžia, ar pasirėmimas teisėto intereso kriterijumi yra tinkamas konkrečiu atveju[48]. Interesų balansavimo testas yra atliekamas tik esant aiškumui dėl visų būtinų sąlygų šio kriterijaus taikymui, t. y. duomenų valdytojo ar trečiojo asmens interesas turi būti teisėtas, realus ir egzistuojantis vertinimo metu, taip pat pakankamai konkretus, kad būtų įmanoma įvertinti interesų balansą[49]. Be to, turi būti nustatyta, kad duomenų tvarkymas yra reikalingas duomenų valdytojo ar trečiojo asmens teisėto intereso įgyvendinimui. Įdomu tai, kad duomenų subjekto interesams, kurie bus gretinami su duomenų valdytojo ar trečiojo asmens interesais, nėra taikomas teisėtumo reikalavimas. Tai reiškia, kad asmenims taikoma platesnė jų interesų ir teisių apsauga, užtikrinanti, kad net ir asmenų, kurie užsiėmė nelegalia veikla, duomenys nebus šiuo pagrindu neproporcingai paviešinti (pavyzdžiui, vagystės atveju nusikaltusio asmens interesai gali būti laikomi viršesniais nei parduotuvės savininko, kuris nori viešai paskelbti nusikaltusio asmens nuotraukas)[50]. Atliekant interesų subalansavimo testą yra vertinamas teisėto intereso šaltinis, būtent, ar duomenų tvarkymas yra reikalingas fundamentalios teisės įgyvendinimui, o galbūt jis atitinka viešąjį interesą ar kitaip teikia naudą visuomenei. Taip pat vertinamas galimas poveikis duomenų subjektui, t. y. ar tvarkytini duomenys yra jautri nevieša informacija, ar vis dėlto įgyta iš viešai prieinamų šaltinių, taipogi, kokiu būdu bus tvarkomi duomenys (jie

[47] 29 straipsnio duomenų apsaugos darbo grupės 2011 m. liepos 13 d. priimta „Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties“, 01197/11/LT WP187, 2011, p. 34. Duomenų valdytojų informacija, kurią prieš gaunant duomenų subjekto sutikimą būtina pateikti, yra įvardijama 95/46/EB direktyvos 10 ir 11 straipsniuose (arba ADTAĮ 24 str.).
[48] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, 2014, p. 9.
[49] *Ibid.,* p. 25.
[50] *Ibid.,* p. 30.

atskleidžiami viešai ar gretinami su kitais duomenimis, pavyzdžiui, sudarant asmens profilį reklamos tikslais), įvertinami ir duomenų subjekto statusas (ar duomenų subjektas yra labiau pažeidžiamas duomenų valdytojo ar trečiojo asmens atžvilgiu, pavyzdžiui, yra vaikas) bei pagrįsti lūkesčiai. Pagaliau, žiūrima, ar bus naudojamos papildomos apsaugos priemonės, kurios padėtų išvengti pernelyg didelio poveikio duomenų subjektui, o tai yra duomenų tvarkymo minimizavimas (pavyzdžiui, nustatant aiškų limitą renkamai informacijai), techninės ir organizacinės priemonės, siekiant įsitikinti, kad surinktų duomenų pagrindų nebus priimami jokie sprendimai, naudojamos technologijos, kurios užtikrintų didesnę duomenų apsaugą, didelis skaidrumo laipsnis[51]. Jei atliktu testu bus nustatyta, kad duomenų subjekto interesai nėra svarbesni nei duomenų valdytojo ar trečiojo asmens interesai, tai šio subjekto asmens duomenys galės būti tvarkomi teisėtų interesų pagrindu.

3. *Ypatingųjų asmens duomenų tvarkymo ypatybės*

Turint omenyje aptartus duomenų tvarkymo kriterijus, svarbu atsižvelgti ir į ypatingųjų asmens duomenų[52] tvarkymo reguliavimą. Ypatingieji asmens duomenys savo pobūdžiu yra laikomi slaptais, todėl jų tvarkymas paprastai yra draudžiamas. Vis dėlto, kai kuriais atvejais yra taikomos išimtys (jos išvardytos ADTAĮ 5 str. 2 d.), ir viena iš jų yra ypatingųjų asmens duomenų tvarkymas gavus duomenų subjekto sutikimą (ADTAĮ 5 str. 2 d. 1 p.). Kadangi teisės aktai ypatingiesiems asmens duomenims taiko didesnę apsaugą, tai natūralu, kad duomenų subjekto sutikimo davimo atveju taip pat yra taikomi griežtesni reikalavimai. ADTAĮ 2 str. 12 punkte yra įtvirtinta, kad sutikimas tvarkyti ypatingus asmens duomenis turi būti išreikštas aiškiai – rašytine, jai prilyginta ar kita forma, neabejotinai įrodančia duomenų subjekto valią. Sąvoka „aiškus sutikimas“ (angl. *express consent* arba *explicit consent*) apima atvejus, kai „asmenims pateikiamas pasiūlymas sutikti arba nesutikti, kad jų asmeninė informacija būtų konkrečiai naudojama ar atskleidžiama, ir jie aktyviai, žodžiu arba raštu, atsako į šį klausimą“[53]. Elektroninėje erdvėje aiškus sutikimas gali būti duodamas naudojant elektroninį ar skaitmeninį parašus, taip pat toks sutikimas bus laikomas duotu ir nuspaudus mygtuką interneto svetainėje, išsiunčiant patvirtinamąjį elektroninį laišką ar pan. Tačiau atkreiptinas dėmesys, kad

[51] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, 2014, p. 50 - 51.
[52] Ypatingi asmens duomenys – duomenys, susiję su fizinio asmens rasine ar etnine kilme, politiniais, religiniais, filosofiniais ar kitais įsitikinimais, naryste profesinėse sąjungose, sveikata, lytiniu gyvenimu, taip pat informacija apie asmens teistumą (ADTAĮ 2 str. 8 p.).
[53] 29 straipsnio duomenų apsaugos darbo grupės 2011 m. liepos 13 d. priimta „Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties“, 01197/11/LT WP187, 2011, p. 24.

prireikus įrodyti aiškaus sutikimo faktą „sutikimas, kuris turi būti gautas nuspaudus mygtuką, patvirtinus asmens tapatybę e. pašto adresu, turės daug mažesnę įrodomąją vertę, nei panašus procesas, paremtas, pvz., įrašomo sutikimo mechanizmais“[54]. Aktualu yra apžvelgti aukščiau aptartų teisėtų duomenų valdytojo ar trečiojo asmens interesų bei ypatingųjų asmens duomenų santykį. Šiuo atveju galimi du požiūriai: pirmas, kad ADTAĮ 5 str. 2 dalyje dėl ypatingųjų asmens duomenų yra įtvirtinta specialioji taisyklė, kuri lemia, jog ypatingieji asmens duomenys gali būti tvarkomi neatsižvelgiant į ADTAĮ 5 str. 1 d. 6 punktą (t. y. teisėtus interesus); antras, kad išvardinti galimi ypatingųjų duomenų tvarkymo atvejai, tik nustato konkrečias išimtis iš draudimo juos tvarkyti, tačiau nenustato pakankamo teisinio duomenų tvarkymo pagrindo[55]. Jau buvo minėta, kad ypatingiesiems asmens duomenims yra taikoma didesnė teisinė apsauga, pavyzdžiui, aptartas aiškaus sutikimo reikalavimas, tačiau pažymėtina, kad tam tikrais aspektais ADTAĮ 5 str. 2 dalyje nustatytos išimtys nėra savaime griežtesnės nei ADTAĮ 5 str. 1 d. išdėstyti reikalavimai. Pavyzdžiui, ADTAĮ 5 str. 2 d. 5 punkte yra įtvirtinta, kad ypatingieji asmens duomenys gali būti tvarkomi, jei duomenų subjektas juos paskelbė viešai. Atsižvelgus į visuminį ypatingųjų asmens duomenų statusą, jų apsaugos priežastis ir tikslus, būtų klaidinga leisti viešai paskelbtų ypatingųjų asmens duomenų tvarkymą, neįvertinus interesų balanso pagal ADTAĮ 5 str. 1 d. 6 punktą[56]. Taigi, susidūrus su asmens ypatingaisiais duomenimis ir ypač siekiant juos teisėtai tvarkyti, reikia atkreipti dėmesį ne tik į papildomus reikalavimus, bet ir įstatymų leidėjo tikslus, kuriant minėtus reikalavimus.

Iš šiame darbo skyriuje aptartos informacijos galima padaryti porą svarbių įžvalgų apie elektroninėje erdvėje vykdomas duomenų tvarkymo procedūras. Pirma, verslo subjektų vykdomas asmens duomenų tvarkymas elektroninėje erdvėje (tuo atveju, kai iniciatyvą tvarkymui rodo ne pats duomenų subjektas) paprastai atliekamas dviem pagrindais: remiantis duomenų valdytojo teisėtu interesu ar duomenų subjekto sutikimu. Antra, tuo atveju, kai asmens duomenų tvarkymas internete nėra būtinas verslo subjekto teisėto intereso įgyvendinimui (t. y. būtinas siūlomos paslaugos įgyvendinimui), verslo subjektas privalo iš vartotojo gauti jo sutikimą asmens duomenų tvarkymui. O tuo atveju, kai tvarkomi ypatingieji asmens duomenys, duomenų subjekto sutikimas turi būti itin aiškiai išreikštas. Kadangi asmens duomenų tvarkymo būtinumas nėra toks jau dažnas

[54] 29 straipsnio duomenų apsaugos darbo grupės 2011 m. liepos 13 d. priimta „Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties“, 01197/11/LT WP187, 2011, p. 25.
[55] Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN WP 217, 2014, p. 14.
[56] Tokios nuomonės laikosi ir 29 straipsnio duomenų apsaugos darbo grupė (žr. *ibid.*, p. 15).

reiškinys, duomenų subjekto sutikimas tampa esminiu asmens duomenų tvarkymo pagrindu. Šie ypatumai iš dalies paaiškina, kodėl teisinėse diskusijose asmens duomenų elektroninėje erdvėje tvarkymo klausimais tiek daug dėmesio yra skiriama būtent asmens sutikimui. Ir kartu paaiškina, kodėl kai kuriais atvejais asmens duomenų tvarkymui duomenų subjekto sutikimas nėra reikalingas.

1.4 Taikytinos teisės problematika

Tokios elektroninės erdvės savybės kaip fizinių ribų nebuvimas, globalumas sukelia tam tikras problemas taikytinos teisės srityje. Asmens duomenų tvarkymas internete vis dažniau tampa tarptautine veikla, kur sunku nustatyti atskirose šalyse esančių duomenų valdytojų veiklą ir atsakomybes. Minėtas neapibrėžtumas, o kartu ir skirtingas atskirų valstybių požiūris į taikytiną teisę panašiose situacijose, sudaro sąlygas valstybių teisės kolizijoms. Be to, taikytinos teisės klausimai yra itin svarbūs tiek duomenų valdytojams, tiek duomenų subjektams. Atsižvelgiant į tai, kad asmens duomenų tvarkymui internete ir fizinėje erdvėje taikoma atskirų valstybių narių nacionalinė teisė, asmens duomenų valdytojai turi aktyviai domėtis, kurios būtent šalies teisė yra taikoma jų veiklai. Tuo tarpu duomenų subjektams aktualu žinoti, ar visi duomenų valdytojai internete su jų duomenimis elgsis vienodai. Pažymėtina, kad asmens duomenų tvarkymas internete yra sąlyginai naujas reiškinys, kurio teisinis reguliavimas formuojasi kartu su besiplečiančiomis interneto galimybėms ir didėjančiu interneto vartotojų pasiekiamumu. Todėl ir teisės taikymo klausimai šioje srityje yra pakankamai nauji bei probleminiai.

Direktyvos 95/46/EB 4 str. 1 dalies a) punkte įtvirtinta bendra taisyklė, kad taikytina teisė priklauso nuo duomenų valdytojo padalinio veiklos vykdymo vietos. Atkreiptinas dėmesys, kad internete, kur duomenų judėjimo dažnu atveju neriboja valstybių teritorijos, tokią veiklos vykdymo vietą nustatyti gali būti sudėtinga. Europos Sąjungos Teisingumo Teismas konkretizavo šią taisyklę *Google Spain* ir *Google* byloje[57], nurodydamas, kad asmens duomenys yra tvarkomi duomenų valdytojo padaliniui vykdant veiklą valstybės narės teritorijoje, jei duomenų valdytojas įsteigia valstybėje narėje savo filialą arba dukterinę bendrovę, kurių veikla orientuojama į tos valstybės gyventojus. Byloje taip pat buvo patikslinta duomenų valdytojo padalinio samprata. Teisingumo Teismas padarė nuorodą į direktyvos 95/46/EB 19 punktą konstatuojamoje dalyje ir pagal tai sprendė, kad padaliniu turi būti laikomas veiksmingą ir realią veiklą vykdantis

[57] Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain and Google* C-131/12, ECLI:EU:C:2014:317.

nuolatinis vienetas tam tikros valstybės narės teritorijoje, turintis teisinį subjektiškumą. Svarbus aspektas, kurį minėtoje byloje nurodė Teisingumo Teismas, yra tas, kad taikytinos teisės nustatymui nėra būtina, jog pats padalinys atliktų asmens duomenų tvarkymą. Užtenka, kad asmens duomenų tvarkymas būtų atliekamas padaliniui vykdant susijusią veiklą. Nustatant, ar veikla yra susijusi su asmens duomenų tvarkymu, vertinama padalinio veiklos prigimtis (t. y. įvertinama, kokia veikla vykdoma ir kokie duomenys renkami)[58]. Konkrečiu atveju Teisingumo Teismas pripažino, kad *Google* padalinys Ispanijoje, kuris užsiėmė reklaminių pranešimų vietų internete pardavimu ir rinkodara, vykdė su asmens duomenų tvarkymu susijusią veiklą. Paminėtina, kad toks Teisingumo Teismo sprendimas susilaukė ir kritikos, kadangi su asmens duomenų tvarkymu susijusia veikla buvo galimai pripažintas visas interneto paieškos variklių verslo modelis. Tai yra, interneto paieškos varikliai gauna pajamas iš parduodamų vietų reklamai, o pajamų gavimas iš vienos pusės ir sudaro sąlygas asmens duomenų tvarkymui. Tačiau klausimas, ar pajamų, sudarančių sąlygas asmens duomenų tvarkymui, gavimas visais atvejais gali būti laikomas veikla, susijusia su asmens duomenų tvarkymu, lieka atviras[59]. Taigi, remiantis *Google Spain* ir *Google* byla, galima apibendrinti, kad tuo atveju, kai ES arba Europos Ekonominės Erdvės valstybėje narėje veikia duomenų valdytojo padalinys, jo veiklai taikytina teisė bus apsprendžiama pagal padalinio įsisteigimo vietą, veiklos prigimtį ir jos vykdymo vietą.

Dar vienas Teisingumo Teismo sprendimas, susijęs su taikytinos teisės klausimais, buvo priimtas *Weltimmo* byloje, kur buvo pasisakyta dėl padalinio sąvokos aprėpties[60]. Nagrinėjamu atveju įmonė pavadinimu *Weltimmo* buvo įsiregistravusi Slovakijoje. Ši įmonė eksploatavo nekilnojamojo turto interneto svetainę, kurioje vengrų kalba buvo talpinami skelbimai apie Vengrijoje esantį nekilnojamąjį turtą. Taip pat ši įmonė Vengrijoje turėjo savo atstovą, kuris buvo įrašytas į Slovakijos įmonių registrą kaip turintis adresą Vengrijoje. Teisingumo Teismas nusprendė, kad šiuo atveju byloje turi būti taikoma Vengrijos teisė. Teismas nurodė, kad padalinio teisinė forma nėra lemiamas veiksnys, taigi Vengrijoje esantis atstovas, atsižvelgiant į kitas sąlygas, taip pat laikytinas padaliniu. Direktyvos 95/46/EB 4 str. 1 d. a) punktas aiškintinas taip, kad pagal jį leidžiama taikyti kitos nei ta, kur asmens duomenų valdytojas registruotas, valstybės narės teisės aktus dėl asmens duomenų apsaugos, jeigu šis valdytojas per nuolatinį

[58] 29 straipsnio duomenų apsaugos darbo grupės 2010 m. gruodžio 16 d. priimta „Nuomonė 8/2010 dėl taikytinos teisės“, 0836-02/10/LT, WP179, 2010, p. 13.
[59] BRKAN, M. Data Protection and Conflict-of-laws: A Challenging Relationship. *European Data Protection Law Review*, 2016, vol. 2, p. 327.
[60] Europos Sąjungos Teisingumo Teismas. 2015 m. spalio 1 d. sprendimas *Weltimmo* C-230/14, ECLI:EU:C:2015:639,

vienetą tos valstybės narės teritorijoje veiksmingai ir realiai vykdo bent minimalią veiklą. Teisingumo Teismas taip pat pažymėjo, kad nacionalinis teismas byloje, spręsdamas dėl taikytinos teisės, gali atsižvelgti į tai, ar padalinio veikla yra skirta konkrečiai valstybės narei. Tačiau atkreipė dėmesį, jog su šiuo duomenų tvarkymu susijusių asmenų pilietybė nėra reikšminga. Šiuo sprendimu Teisingumo Teismas įtvirtino lanksčią padalinio sąvokos sampratą ir atmetė formalų požiūrį, kad įmonė gali būti įsteigta, kaip tai suprantama direktyvoje 95/46/EB, tik savo teisinės registracijos vietoje.

Tuo atveju, jeigu duomenų valdytojas neturi padalinio, veikiančio valstybėje narėje, taikytinos teisės nustatymui bus naudojami direktyvos 95/46/EB 4 str. 1 d. b) arba c) punktai. Direktyvos 4 str. 1 d. b) punktas yra skirtas tiems atvejams, kai nacionalinė duomenų apsaugos teisė gali būti taikoma ir už tos valstybės sienų. Pavyzdžiui, remiantis tarptautinės teisės normomis ar tarptautiniais susitarimais, nacionalinė duomenų apsaugos teisė gali būti taikoma ambasadai ar konsulatui, taip pat laivui ar lėktuvui[61]. Atsižvelgiant į šią specifiką, straipsnio 1 dalies b) punkto nuostatos praktikoje nėra dažnai naudojamos. Tuo tarpu direktyvos 95/46/EB 4 str. 1 d. c) punktas taip pat apima atvejus, kai duomenų valdytojas neturi padalinio veikiančio valstybėje narėje. Tačiau jeigu trečiosios šalies duomenų valdytojas asmens duomenų tvarkymui naudoja įrangą, esančią valstybės narės teritorijoje, tai jam bus taikoma tos valstybės narės teisė. Teisinėje literatūroje atkreipiamas dėmesys, kad taikytinos teisės priklausomybės nuo valstybėje esančios įrangos koncepcija yra gana paini. Šiuo atveju nėra aišku, kokia būtent įranga turima omenyje – ar tai gali būti tik techninė, ar ir programinė įranga, ar ji turi būti skirta asmens duomenų tvarkymui, ar gali būti tiesiog susijusi su šia veikla[62]. Darbo grupė atsakymus į dalį šių klausimų interpretuoja plačiai, nurodo, kad sąvoka „įranga“ turėtų reikšti „priemones“, kurios apimtų tiek tarpininkaujantį personalą ar techninę įrangą, tiek programinę įrangą, ir pavyzdžiui, net slapukus[63]. Toks traktavimas yra itin platus ir suponuojantis, kad net ir menkiausiai veiklai, net ir nenukreiptai į ES vartotojus, gali būti taikomos 95/46/EB direktyvos nuostatos. Vis dėlto, trūkstant teismų praktikos šiuo klausimu, yra sunku pasakyti, ar teismai būtų linkę įrangą traktuoti itin plačiai, ir apskritai, kokiais atvejais ir kokia apimtimi direktyvos 4 str. 1 d. c) punktas tiksliai turėtų būti taikomas.

[61] 29 straipsnio duomenų apsaugos darbo grupės 2010 m. gruodžio 16 d. priimta „Nuomonė 8/2010 dėl taikytinos teisės“, 0836-02/10/LT, WP179, 2010, p. 17.
[62] BRKAN, M. Data Protection and Conflict-of-laws: A Challenging Relationship. *European Data Protection Law Review*, 2016, vol. 2, p. 326.
[63] 29 straipsnio duomenų apsaugos darbo grupės 2010 m. gruodžio 16 d. priimta „Nuomonė 8/2010 dėl taikytinos teisės“, 0836-02/10/LT, WP179, 2010, p. 20.

ADTAĮ 1 str. 3 dalies nuostatos iš esmės atitinka aukščiau aptartą 95/46/EB direktyvos reguliavimą taikytinos teisės srityje. Jas nagrinėjant turėtų būti keliamos tos pačios problemos, todėl atskirai jas šioje dalyje aptarti yra netikslinga. Apibendrinant galima paminėti, kad, kaip ir dauguma nuostatų 95/46/EB direktyvoje, taikytiną teisę reguliuojančios taisyklės yra orientuotos į asmens duomenų tvarkymą fizinėje, o ne elektroninėje erdvėje. Iš dalies dėl to Teisingumo Teismas, atsižvelgdamas į globalizaciją ir šiuolaikines technologijas, yra priverstas šias taisykles aiškinti itin plečiamai. Tuo aspektu Europos Komisijos dar 2012 metais inicijuota duomenų apsaugos reforma, žadanti aiškų ir modernų visapusišką reguliavimą, yra labai laukiama. Toliau darbe bus apžvelgiamos minėtos reformos žadamos naujovės, susikoncentruojant į 95/46/EB direktyvą iš esmės keičiančio teisės akto ypatybes.

2. ES DUOMENŲ APSAUGOS TEISINĖS SISTEMOS REFORMA ELEKTRONINĖS ERDVĖS KONTEKSTE

Kai kuriose pirmosios darbo dalies vietose buvo atkreiptas dėmesys, kad direktyvos 95/46/EB nuostatos turi nemažai neaiškumų ir trūkumų, kurie labiausiai pastebimi direktyvą taikant asmens duomenų apsaugai būtent elektroninėje erdvėje. Ir tai nėra stebėtina, turint omenyje, kad direktyva 95/46/EB buvo priimta 1995 metais. Atsižvelgiant į skaitmeninės aplinkos dinamiškumą ir radikalius pokyčius, vykusius elektroninėje erdvėje nuo devyniasdešimtųjų metų vidurio, minėtą direktyvą beveik galima pavadinti „atgyvenusia“. Kartu paminėtina, kad pastarieji du dešimtmečiai kartu su technologine pažanga, be kita ko, atnešė ir papildomas rizikas, susijusias su asmenų privatumu, kurios iš esmės pakeitė asmens duomenų tvarkymo principus. Be to, interneto sąlygota globalizacija sudarė itin palankias sąlygas duomenų judėjimui tarp valstybių, o tai iškėlė naujus klausimus dėl direktyvos 95/46/EB nuostatų taikymo kitose jurisdikcijose[64]. Europos Komisijos nuomone, dar vienas dabartinio teisinio reguliavimo trūkumas yra tarpusavyje nederanti ir fragmentiška teisinė aplinka, sudariusi sąlygas teisiniam netikrumui ir nevienodo lygio asmens duomenų apsaugai skirtingose valstybėse[65]. 2012 m. sausio 25 d. Europos Komisija visas šias problemas pabandė išspręsti, pasiūlydama Europos Sąjungai iš esmės reformuoti 1995 metais įtvirtintas asmens duomenų apsaugos taisykles. Europos Komisijos pasiūlyti pakeitimai buvo svarstomi beveik keturis metus – iki 2015 metų gruodžio mėnesio[66]. Pagaliau, buvo pasiektas susitarimas, ir 2016 metų balandį Europos Sąjungos Taryba ir Europos Parlamentas priėmė reglamentą (ES) 2016/679 „dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)“ (toliau ir – Bendrasis duomenų apsaugos reglamentas, BDAR)[67]. Bendrasis duomenų apsaugos reglamentas bus pradėtas taikyti nuo 2018 m. gegužės 28 d..

---

[64] BURRI, M., SCHÄR, R. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 2016, vol. 6, p. 480.

[65] European Commision. Commission Staff Working Paper Executive Summary Of The Impact Assessment. Brussels, SEC(2012) 73 final, 2012, p. 2.

[66] Tiek žiniasklaidoje, tiek teisinėje literatūroje atkreipiamas dėmesys, kad Europos Komisijos pasiūlytą reformą lydėjo gana agresyvios lobistinės iniciatyvos iš suinteresuotų verslo bei visuomenės grupių, taip pat ir Europos Sąjungos pagrindinių institucijų nesutarimai įvairiausiais klausimais.

[67] Kartu su BDAR buvo priimta 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. Kaip ir pasakyta pačiame pavadinime, ši direktyva reguliuos fizinių asmenų apsaugą būtent kompetentingoms institucijoms tvarkant asmens duomenis nurodytais tikslais. Minėta direktyva į nacionalinę teisė turi būti perkelta iki 2018 m. gegužės 6 d. Atsižvelgiant į tai, kad šiame darbe

Prieš apžvelgiant asmens duomenų apsaugos reguliavimo pokyčius, kurie įtvirtinti naujajame BDAR, turinio aspektu, svarbu paminėti ir pakitusią reguliavimo formą. Direktyva 95/46/EB yra pakeičiama reglamentu, o tai reiškia, kad suėjus terminui šis reglamentas automatiškai taps valstybių narių nacionalinių teisės sistemų dalimi. Taigi, šis reglamentas valstybėse narėse turės teisinį poveikį nepriklausomai nuo jų nacionalinės teisės, ir valstybės narės lokaliais aktais negalės užgožti reglamento nuostatų[68]. Iki šiol reglamentai būdavo naudojami labiau savarankiškose, atribotose srityse kaip konkurencijos teisė, ES agentūrų steigimas ir valdymas ar su ES prekės ženklu susijęs reguliavimas ir pan. Kitose srityse, parenkant reguliavimo formą, pirmenybė būdavo suteikiama direktyvoms, paliekant galimybę valstybėms narėms jas savarankiškai įgyvendinti. Tai, kad šiuo atveju asmens duomenų apsaugos reguliavimui buvo pasirinktas būtent reglamentas, leidžia spręsti apie įvykusį kokybinį pokytį – duomenų apsauga ES nebėra traktuojama kaip lokalus reiškinys, kurį valstybės narės gali reguliuoti nacionaliniais aktais[69]. Priešingai, toks pasirinkimas atskleidė, kad duomenų apsauga tapo visos Europos Sąjungos rūpesčiu ir privalo būti reguliuojama vienodai visose valstybėse narėse. Bendrasis duomenų apsaugos reglamentas vien jau savo forma garantuoja aukštesnio lygio teisinę harmonizaciją ir užtikrina mažesnį skaičių nesutapimų atskirų valstybių narių reguliavime. Kartu reglamento priėmimą galima traktuoti kaip bandymą paauklėti tam tikras valstybes nares dėl jų itin švelnaus požiūrio į duomenų apsaugos taisyklių taikymą praktikoje[70].

Be abejo, BDAR priėmimas taip pat reiškia, kad iki jo taikymo pradžios visų ES institucijų laukia gana įtemptas laikotarpis, per kurį turės būti pasiruošta naujo reguliavimo įgyvendinimui. Nacionaliniai aktai (tokie kaip ADTAĮ) turės būti panaikinami arba adaptuojami taip, kad reguliavimas nesidubliuotų su BDAR ar jam neprieštarautų. Atitinkamai turės būti koordinuojama visų valstybių narių duomenų apsaugos įgyvendinimo priežiūra, nacionalinių teismų sprendimai susijusiais klausimais ir kt. Ir čia tik kalbant apie pokyčius, apspręstus naujo reglamentavimo formos, o ne turinio. Direktyvoje 95/46/EB esantys 34 straipsniai yra pakeičiami beveik šimtu BDAR straipsnių, taigi medžiagos mokslinei analizei asmens duomenų apsaugos klausimais yra

---

yra koncentruojamasi į bendras asmens duomenų tvarkymo taisykles, kurios nėra glaudžiai susijusios su duomenų tvarkymu veikiant išimtinai kompetentingoms institucijoms, Europos Parlamento ir Tarybos direktyva (ES) 2016/680 išsamiau darbe aptarta nebus.

[68] CRAIG, P., BURCA, G. EU Law: Text, cases and materials. Sixth Edition. New York: Oxford University Press, 2015, p. 107.

[69] HERT, P., PAPAKONSTANTINOU, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, 2016, vol. 32(2), p. 182.

[70] BURRI, M., SCHÄR, R. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 2016, vol. 6, p. 489.

daugiau nei pakankamai. Toliau bus bandoma paanalizuoti svarbiausius BDAR turinio pokyčius, kiek tai nenutolsta nuo pagrindinės darbo temos. Nagrinėjami klausimai, be kita ko, apima ir pokyčius asmens duomenų sampratoje, duomenų tvarkyme bei naujoves taikytinoje teisėje.

1. *Asmens duomenų sampratos patikslinimas*

Bendrajame duomenų apsaugos reglamente naudojamas iš esmės tas pats asmens duomenų apibrėžimas kaip ir 95/46/EB direktyvoje. Tačiau naujajame dokumente aiškiau įvardijama, kas yra laikoma asmeniu, kurio tapatybė gali būti nustatyta[71]. Į tokio asmens apibrėžimą įtraukiama nauja sąvoka „interneto identifikatoriai“, kuri smulkiau apibūdinama reglamento konstatuojamosios dalies 30 punkte. Šis punktas nustato, kad interneto identifikatoriais turėtų būti laikomi IP adresai, slapukų identifikatoriai arba kiti identifikatoriai, pavyzdžiui, radijo dažninio atpažinimo žymenys. BDAR įtvirtintame asmens duomenų apibrėžime yra ir toliau laikomasi išplėstinio požiūrio į asmens duomenų sąvoką, kuris buvo nuosekliai plėtojamas šiame darbe jau nagrinėtoje Darbo grupės nuomonėje dėl asmens duomenų sąvokos (4/2007) ir kai kuriuose Teisingumo Teismo sprendimuose[72]. Interneto identifikatorių sąvokos įtraukimas į asmens duomenų apibrėžimą buvo nuspėjamas, tačiau teigiamas žingsnis, atliktas siekiant sąvokos išsamumo.

2. *Pokyčiai asmens duomenų tvarkymo reguliavime*

Bendrasis duomenų apsaugos reglamentas įtvirtina nemažai pasikeitimų, susijusių su asmens duomenų tvarkymu elektroninėje erdvėje. Pirmiausia, prie pirmoje darbo dalyje minėtų duomenų kokybės principų yra prijungiami vientisumo, konfidencialumo, skaidrumo ir atskaitomybės principai. Vienu iš svarbiausių – skaidrumo principu – yra siekiama sukurti pasitikėjimu grįstą duomenų tvarkymo aplinką, kuri padėtų panaikinti nemalonų įspūdį, kad asmens duomenys paprastai tvarkomi slaptai, už uždarų durų. Tuo tarpu atskaitomybės principas įtrauktas siekiant duomenų valdytojams priskirti

[71] Fizinis asmuo, kurio tapatybę galima nustatyti – tai asmuo, kurio tapatybę tiesiogiai arba netiesiogiai galima nustatyti, visų pirma pagal identifikatorių, kaip antai vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius (BDAR 4 str. 1 punktą).

[72] Pavyzdžiui, Europos Sąjungos Teisingumo Teismo 2011 m. lapkričio 24 d. sprendime *Scarlet Extended,* C‑70/10 buvo nustatyta, kad statiniai interneto vartotojų IP adresai yra saugomi asmens duomenys, nes leidžia tiksliai nustatyti tokius vartotojus (žr. šios sprendimo 51 punktą). Taip pat, Europos Sąjungos Teisingumo Teismo 2016 m. spalio 19 d. sprendime *Patrick Breyer / Bundesrepublik Deutschland* C‑582/14 buvo pripažinta, kad ir dinaminiai IP adresai, net kai elektroninių paslaugų teikėjas neturi papildomos informacijos, būtinos vartotojų tapatybei nustatyti, turi būti laikomi asmens duomenimis (žr., be kita ko, 48-49 minėto sprendimo punktus).

atsakomybę dėl specifinių priemonių, užtikrinančių duomenų apsaugos reikalavimus, įgyvendinimo. Naujų priemonių reglamente pavyzdžiai gali būti pareiga, esant tam tikroms sąlygoms, paskirti duomenų apsaugos pareigūną, poreikis atlikti poveikio duomenų apsaugai vertinimą ir pan.[73]. Bendrai paėmus, reglamente įtvirtinti duomenų tvarkymo principai esmingai nesiskiria nuo 95/46/EB direktyvoje pateiktų principų (reglamente jie tik įvardijami aiškiau). Tai, kad pagrindiniai teisėto duomenų tvarkymo principai per pastaruosius dvidešimt metų esmingai nepasikeitė leidžia spręsti apie jų lankstumą ir atsparumą, o kartu ir apie tam tikrą duomenų apsaugos politikos nuoseklumą.

Antra, Bendrajame duomenų apsaugos reglamente patikslinami reikalavimai duomenų valdytojui, kuris siekia gauti duomenų subjekto sutikimą dėl asmens duomenų tvarkymo. Toks patikslinimas yra svarbus, kadangi atskiros nacionalinės priežiūros institucijos buvo linkusios skirtingai interpretuoti duomenų subjektų sutikimus ir jų gavimo būdus. Darbo grupės nuomonėje dėl sąvokos „sutikimas“ apibrėžties (15/2011) buvo nurodytos pagrindinės taisyklės, taikytinos norint gauti duomenų subjekto sutikimą (apie tai buvo kalbėta pirmoje darbo dalyje). Tačiau ši nuomonė nėra privalomas teisės aktas (tai *soft law* šaltinis), todėl susidarydavo situacija, kai vienoje valstybėje narėje teisėtai gautas ir galiojantis sutikimas galėjo neturėti teisinės galios kitoje valstybėje[74]. Naujajame reglamente prie duomenų subjekto sutikimo sąvokos[75] pridedamas reikalavimas dėl konkretumo, o taip pat dėl duomenų subjekto pareiškimo ar vienareikšmiškų veiksmų. Konstatuojamos BDAR dalies 32 punkte smulkiau nurodoma, kad asmens sutikimas turi būti duodamas aiškiu, patvirtinančiu veiksmu, pavyzdžiui, raštišku, įskaitant elektronines priemones, ar žodiniu pareiškimu. Nurodoma, kad tai galėtų būti atliekama pažymint langelį interneto svetainėje, pasirenkant informacinės visuomenės paslaugų techninius parametrus arba kitu pareiškimu arba poelgiu, iš kurio aiškiai matyti tame kontekste, kad duomenų subjektas sutinka su siūlomu jo asmens duomenų tvarkymu. Tai reiškia, kad nebeveiksmingos bus praeityje duomenų valdytojų naudotos gudrybės, siekiant gauti asmenų sutikimus dėl duomenų tvarkymo, pavyzdžiui, iš anksto laukelyje pažymėta varnelė ar numanomas (angl. *implied)* sutikimas tuo atveju, jei tarp asmens ir duomenų valdytojo susiklosto sutartiniai santykiai. BDAR 7 straipsnio

[73] HERT, P., PAPAKONSTANTINOU, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, 2016, vol. 32(2), p. 134.
[74] REDING, V. The European data protection framework for the twenty-first century. *International Data Privacy Law*, Oxford University Press, 2012, vol. 2, No. 3, p. 124.
[75] Duomenų subjekto sutikimas – bet koks laisva valia duotas, konkretus ir nedviprasmiškas tinkamai informuoto duomenų subjekto valios išreiškimas pareiškimu arba vienareikšmiais veiksmais kuriais jis sutinka, kad būtų tvarkomi su juo susiję asmens duomenys (pagal BDAR 4 str. 11 punktą).

1 dalis nurodo, kad atsakomybė dėl asmens sutikimo egzistavimo įrodymo pilna apimtimi tenka duomenų valdytojui. To paties straipsnio 3 dalis įveda dar vieną naujovę, t. y. nustato duomenų subjektui teisę bet kuriuo metu atšaukti savo sutikimą (deja, ši teisė neturės retrospektyvinės galios). Pažymėtina, kad BDAR 8 straipsnis numato, jog asmens, jaunesnio nei 16 metų, duomenų tvarkymas yra teisėtas tik tuo atveju, jeigu sutikimą davė arba tvarkyti duomenis leido vaiko tėvų pareigų turėtojas. Taigi, priešingai nei buvusiame teisiniame reguliavime, naujasis reglamentas pripažįsta, kad vaiko asmens duomenys turi turėti specifinę apsaugą[76]. Turint omenyje, kad didžioji dalis asmens duomenų tvarkymo elektroninėje erdvėje yra paremta būtent sutikimo iš duomenų subjekto gavimu, šios pristatytos naujovės yra tikrai aktualios.

3. *Dėl skirtingo asmenį identifikuojančių ir potencialiai identifikuojančių duomenų traktavimo*

Pirmoje darbo dalyje buvo kalbėta apie tai, kad asmens duomenys gali tiek identifikuoti asmenį (angl. *identified natural person*), tiek potencialiai identifikuoti asmenį, apjungus juos su kita informacija (angl. *identifiable natural person*). Ši atskirtis yra išlaikoma naujajame reglamente, kartu padedant pagrindus skirtingam šių kategorijų duomenų traktavimui juos tvarkant. Taigi reglamentu bandoma spręsti 95/46/EB direktyvoje egzistavusi problema dėl tų pačių reikalavimų ir apsaugos lygio taikymo skirtingomis savybėmis pasižymintiems duomenims. Konkrečiai, į BDAR tekstą yra inkorporuojamas pseudonimų suteikimas[77] (angl. *pseudonymisation*) ir 11 straipsnis dėl duomenų tvarkymo, kai asmens tapatybės nustatyti nereikia, kurių 95/46/EB direktyvoje nebuvo. Pseudonimų suteikimas leidžia užtikrinti didesnę apsaugą tvarkant asmenų duomenis, kadangi jo tikslas yra išvengti tiesioginės jungties tarp turimų duomenų ir konkretaus duomenų subjekto tapatybės[78]. Duomenys, kuriems suteikti pseudonimai, nelaikytini anoniminiais duomenimis[79], kadangi duomenų valdytojas duomenų subjektą gali identifikuoti, pasitelkdamas papildomą informaciją (duomenys laikomi anoniminiais,

[76] Daugiau apie vaiko duomenų apsaugą naujame reglamente žr. MACENAITE, M. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New media & society*, 2017, p. 1-15.

[77] Pseudonimų suteikimas – asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskirti konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jos atžvilgiu taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti (pagal BDAR 4 str. 5 punktą).

[78] BOLOGNINI, L., BISTOLF, C. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2016, vol. 33, p. 178.

[79] Atkreipiamas dėmesys, kad, kaip ir 95/46/EB direktyvoje, anoniminių duomenų tvarkymui naujasis reglamentas nėra taikomas (žr. BDAR konstatuojamosios dalies 26 punktą).

kai duomenų subjekto identifikuoti neįmanoma net pasitelkus protingas priemones). Kadangi pseudonimų suteikimas sumažina su duomenų subjektų privatumu susijusias rizikas, reglamente jam taikomi švelnesni reikalavimai. Pavyzdžiui, pseudonimų suteikimas yra viena iš aplinkybių, į kurias atsižvelgiama, kai duomenų valdytojui suteikiama teisė tvarkyti duomenis ne pagal iš anksto nusistatytą tikslą, kuriam tie duomenys buvo surinkti (BDAR 6 str. 4 d. e punktas). Taip pat duomenų, kuriems suteikti pseudonimai, saugumo pažeidimo atveju iš duomenų valdytojo nereikalaujama apie tokį pažeidimą informuoti duomenų subjektą (BDAR 34 str. 3 d. a punktas). Jau minėtas BDAR 11 straipsnis nustato, jog, jeigu dėl tikslų, kuriais duomenų valdytojas tvarko asmens duomenis, duomenų valdytojui nebūtina ar nebėra būtina nustatyti duomenų subjekto tapatybės, duomenų valdytojas nėra įpareigojamas laikyti, gauti ar tvarkyti papildomą informaciją duomenų subjekto tapatybei nustatyti vien tam, kad būtų laikomasi reglamento. Toliau sekančios to paties straipsnio nuostatos nurodo, kad duomenų valdytojui įrodžius, jog jis neturi galimybės nustatyti duomenų subjekto tapatybės, jam netaikomi BDAR 15–20 straipsniai[80]. Taigi, reglamente yra įtvirtintos išimtys iš taisyklių, priklausomai nuo asmens duomenų apdorojimo būdo ir to, ar asmuo pagal turimus duomenis yra jau identifikuotas, ar tik identifikuotinas. Tai rodo, kad rengiant naująjį reglamentą buvo atsižvelgta į duomenų tvarkymo proceso realius techninius parametrus ir galimybes.

4. *Kiti aktualūs pasikeitimai ir papildymai teisiniame reguliavime*

Trumpai verta paminėti pasikeitimus, įtvirtintus naujajame reglamente, susijusius su sustiprėjusiomis vartotojų teisėmis. Viena iš sustiprintų teisių reglamente yra „teisė būti pamirštam“ (angl. *right to be forgotten*), kuri užtikrina galimybę duomenų subjektui pareikalauti, esant tam tikroms sąlygoms, ištrinti visus duomenų valdytojo tvarkomus asmens duomenis. Kartu duomenų valdytojui tenka pareiga informuoti visus kitus to asmens duomenų valdytojus apie privalomą duomenų ar jų kopijų ištrynimą. Taip pat, atsižvelgus į šiandienines realijas, reglamente yra įtraukta profiliavimo sąvoka[81]. Naujame reglamente yra matomi ketinimai sureguliuoti profiliavimą, įtraukiant jį į

[80] BDAR 15–20 straipsniuose įtvirtintos duomenų valdytojų pareigos dėl tvarkomos informacijos prieinamumo bei pateikimo duomenų subjektui reikalaujant, taip pat ištrynimo, ištaisymo ir perkėlimo. Pagal reglamento nuostatas, 15–20 straipsniai netaikomi, išskyrus atvejus, kai duomenų subjektas, siekdamas pasinaudoti pagal šiuo straipsnius jam suteiktomis teisėmis, pateikia papildomos informacijos, leidžiančios nustatyti jo tapatybę.

[81] Profiliavimas – bet kokios formos automatizuotas asmens duomenų tvarkymas, kai asmens duomenys naudojami siekiant įvertinti tam tikrus su fiziniu asmeniu susijusius asmeninius aspektus, visų pirma siekiant išanalizuoti ar numatyti aspektus, susijusius su to fizinio asmens darbo rezultatais, ekonomine situacija, sveikatos būkle, asmeniniais pomėgiais, interesais, patikimumu, elgesiu, buvimo vieta arba judėjimu (pagal BDAR 4 str. 4 punktą).

automatizuotų sprendimų priėmimo kategoriją (BDAR 22 str.). Taigi profiliavimas pagal reglamentą yra leidžiamas, galbūt net remiantis jautriais duomenimis (angl. *sensitive data*)[82], tol, kol užtikrinama atitinkama asmens duomenų apsauga. Visiškai naujai pasirodžiusi yra duomenų subjektų teisė į duomenų perkeliamumą (angl. *right to data portability*), kuri orientuota būtent į interneto (ar tiksliau į socialinių tinklų) vartotojus. Ši teisė reiškia, kad asmenys gali laisvai perkelti savo duomenis iš vieno duomenų valdytojo pas kitą. Tokia naujove bandoma paskatinti atskirų duomenis tvarkančių sistemų tarpusavio sąveiką, o kartu sumažinti kai kurių subjektų dominavimą rinkoje[83]. Kiti reikšmingi pasikeitimai duomenų apsaugos srityje, sąlygoti 95/46/EB direktyvos pakeitimo, apima išaugusią įsipareigojimų, tenkančių tiek duomenų valdytojams, tiek duomenų tvarkytojams, apimtį, itin sustiprintas priežiūros institucijos galias[84].

5. *Naujai reglamentuoti taikytinos teisės klausimai*

Šiuo atveju įdomi yra naujojo reglamento teritorinio taikymo aprėptis, kuri, galima sakyti, iš esmės pakeitė 95/46/EB direktyvoje esančias taisykles, ypač tiems su duomenų tvarkymu susijusiems subjektams, kurie neturi buveinės ES. Viena iš padarytų pakeitimų priežasčių yra ta, kad elektroninėje erdvėje atliekamas asmens duomenų tvarkymas vis labiau nukreipiamas į duomenų subjektus dėl reklaminių paskatų ir siekio parduoti prekes bei paslaugas. Kita priežastis galėjo būti suvokimas, kad duomenų tvarkymas nėra išimtinai susijęs su tam tikra vieta, todėl, tapus vis sunkiau nustatyti tikslią duomenų tvarkymo vietą, prireikė reformuoti patį reguliavimą[85]. Taigi dėl šių priežasčių Bendrajame duomenų apsaugos reglamente taikytiną teisę apspręs ne vien duomenų valdytojų ir tvarkytojų buveinės ir veiklos vykdymo vieta (BDAR 3 str. 1 d.), bet, be kita ko, ir duomenų subjektų buvimo vieta[86]. BDAR 3 str. 2 dalis nustato, kad, duomenų valdytojui ar tvarkytojui neįsisteigus ES, naujasis reglamentas bus taikomas, kai bus tvarkomi ES esančių duomenų subjektų duomenys ir kai tvarkymas bus susijęs su prekių ar paslaugų siūlymu tokiems duomenų subjektams arba elgesio, jiems veikiant ES,

[82] HERT, P., PAPAKONSTANTINOU, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, 2016, vol. 32(2), p. 189.
[83] BURRI, M., SCHÄR, R. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 2016, vol. 6, p. 491.
[84] Nors šie klausimai yra labai aktualūs, bet, atsižvelgus į darbo apimtį, išsikeltą tikslą ir uždavinius, toliau smulkiau aptarinėjami jie nebus.
[85] KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(5), p. 736.
[86] Šiuo atveju duomenų subjektų buvimo vieta turėtų būti suprantama tiek kaip nuolatinė gyvenamoji vieta, tiek kaip gyvenamoji vieta, tiek kaip vieta keliaujant ES, nepriklausomai nuo asmenų pilietybės.

stebėsena[87]. Anksčiau 95/46/EB direktyvoje buvęs kriterijus taikytinai teisei nustatyti, susijęs su automatine ar kitokia įranga, esančia valstybės narės teritorijoje, naujajame reglamente yra panaikinamas. Šis poelgis gali būti siejamas su painia buvusio reguliavimo koncepcija (tiksliai neaišku, kas turi būti laikoma įranga). Taip pat ir su kitais galimais neatitikimais, ypač tais atvejais, kai potencialiai ES duomenų apsaugos taisyklės galėjo būti taikomos net tada, kai duomenų tvarkymas neturi beveik nieko bendro su ES (pavyzdžiui, jei naudojama ES esanti įranga, valdytojas įsisteigęs ne ES valstybėje, tvarkomi ne ES subjektų duomenys)[88]. Vis dėl to, kai kurie autoriai kritikuoja automatinės ar kitokios įrangos kriterijaus pašalinimą nustatant taikytiną teisę. Yra baiminamasi, kad tam tikrų duomenų tvarkymas nepateks į BDAR reguliavimo spektrą ir liks nereguliuojamas apskritai. Šiuo atveju turima omenyje ES esančių asmenų duomenų tvarkymas išmaniosios įrangos (pavyzdžiui, išmaniųjų laikrodžių) pagalba, kai duomenų valdytojas neįsisteigęs ES ir kai tvarkymas yra atliekamas archyvavimo, viešojo intereso arba mokslinio, statistinio, istorinio tyrimo tikslais[89]. Darbo autoriaus nuomone, aprašytas atvejis vis gi turėtų patekti į BDAR reguliavimo sferą pagal 3 str. 2 d. b) punktą, kadangi nurodytu atveju išmaniąja įranga būtų sekamas duomenų subjektų, esančių ES, elgesys. Nors BDAR konstatuojamosios dalies 24 punktas asmens elgesio stebėseną labiau sieja su asmens atsekimu, profilio sudarymu, siekiu analizuoti asmeninius pomėgius ir pan., nėra priežasties, kodėl šiais pavyzdžiais turėtų būti apsiribojama. Praeityje Teisingumo Teismas visuomet buvo linkęs sąvokas, susijusias su duomenų apsauga ir taikytina teise, aiškinti plečiamai (kaip buvo daroma jau aptartose *Google Spain* ir *Weltimmo* bylose). Todėl pozicija, kad automatinės ar kitokios įrangos kriterijaus, nustatant taikytiną teisę, pašalinimas atvėrė spragą asmens duomenų teisiniame reguliavime, turėtų būti vertinama tiesiog kaip prašymas išsamiau išaiškinti tam tikrus su taikytina teise siejamus neatitikimus.

Bendrasis duomenų apsaugos reglamentas moksliniuose straipsniuose vertinamas įvairiai. Vieni autoriai įsitikinę, kad naujasis reguliavimas „pakeis pasaulį“, parodydamas ES kelią iš dabartinės aklavietės duomenų apsaugos srityje ir sukurdamas aukštus

[87] Sąlygos, pagal kurias galima spręsti, ar duomenų subjekto duomenys yra tvarkomi siūlant prekes ir paslaugas yra detalizuotos BDAR konstatuojamosios dalies 23 punkte. BDAR konstatuojamosios dalies 24 punktas detalizuoja, kokia duomenų tvarkymo veikla gali būti laikoma duomenų subjektų elgesio stebėsena.
[88] 29 straipsnio duomenų apsaugos darbo grupės 2010 m. gruodžio 16 d. priimta „Nuomonė 8/2010 dėl taikytinos teisės“, 0836-02/10/LT, WP179, 2010, p. 20.
[89] KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(5), p. 744.

vartotojų teisių standartus bei konkurencingą ir inovatyvią bendrą rinką[90]. Kiti autoriai nurodo, kad BDAR yra mažiausia blogybė, turinti daug potencialo, bet stokojanti realių priemonių, kurios padėtų tą potencialą įgyvendinti[91]. Dažniausiai kritika naujajam reglamentui yra reiškiama dėl per silpnos dabartinės priežiūros institucijų padėties ar vis dar per didelės laisvės, suteikiamos valstybėms narėms, pasireikšti tam tikrais asmens duomenų apsaugos teisės klausimais[92]. Taip pat akcentuojama, kad reglamente nepakankamai aiškiai išdėstoma sąvokų ir procesų reikšmė ir esmė, dėl ko gali būti sunku įgyvendinti kai kuriuos sprendimus. Be to, pats reglamentas, nors atėjus laikui bus taikomas tiesiogiai, yra išdėstytas gana sudėtinga teisine kalba, kurią suprasti asmenims, neturintiems teisinio išsilavinimo, yra sunku[93]. Vis dėlto, reikia sutikti, kad ES duomenų apsaugos teisės srityje įgyvendinta labai svarbi reforma, o jos tikroji įtaka pilna apimtimi atsiskleis pradėjus BDAR taikyti 2018 metais. Naujo reglamento priėmimas yra perspektyvus žingsnis asmens duomenų apsaugai Europos Sąjungoje, kuris turėtų ne tik atskleisti bendrosios skaitmeninės rinkos potencialą, bet ir padėti apsaugoti šiais laikais gana trapų asmenų privatumą.

Asmens duomenų apsaugai šiuo metu taikomų ir tik ką pasirodžiusių teisės aktų nuostatų analizė leidžia susidaryti bendrą vaizdą apie įvairiems subjektams šioje srityje kylančias problemas. Pirmosios dvi darbo dalys buvo orientuotos į iškylančių sunkumų teisinio reguliavimo plotmėje atskleidimą. Likusiose darbo dalyse, bus stengiamasi pažvelgti į teisinio reguliavimo pritaikomumą pasirinktoje reklamos elektroninėje erdvėje srityje. Nagrinėjant konkrečią sritį, darbo pradžioje analizuota medžiaga padės suvokti supančią teisinę aplinką, t. y. įvairių su asmens duomenimis susijusių institucijų išsikeltus tikslus ir galimybes, taip pat vyraujantį požiūrį į asmens duomenų tvarkymą (tvarkymo dar neišskiriant konkrečiai į asmens duomenų rinkimą ir naudojimą). Todėl atlikta teisės aktų apžvalga yra svarbus žingsnis tolesnio temos nagrinėjimo link.

[90] ALBRECHT, J. P. How the GDPR Will Change the World. *European Data Protection Law Review*, 3/2016, vol. 2, p. 289.
[91] DAVIES, S. The Data Protection Regulation: A Triumph of Pragmatism over Principle? *European Data Protection Law Review*, 3/2016, vol. 2, p. 291.
[92] *Ibid.*
[93] BLUME, P. Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*, 2012, vol. 2(3), p. 134.

3. ASMENS DUOMENŲ RINKIMAS IR NAUDOJIMAS VARTOTOJŲ ELGSENA GRĮSTAI REKLAMAI

Europos komisija, pristatydama Bendrąjį duomenų apsaugos reglamentą, savo komunikate nurodė, kad viena iš priežasčių, skatinusių priimti naujas ar pakoreguotas taisykles asmens duomenų teisiniame reguliavime, buvo vartotojų nepasitikėjimas elektronine erdve: „nepasitikintys vartotojai vengia pirkti internetu ir naudotis naujomis paslaugomis. Todėl aukštą duomenų apsaugos lygį būtina užtikrinti ir siekiant padidinti pasitikėjimą internetinėmis paslaugomis bei išnaudoti skaitmeninės ekonomikos potencialą, kartu skatinant ekonomikos augimą ir ES pramonės konkurencingumą“[94]. Europos Komisija vartotojų pasitikėjimą elektronine erdvėje įvardija kaip labai svarbų veiksnį bendros gerovės link. Kyla klausimas, ar šiuo metu egzistuojanti teisinė aplinka, reguliuojanti įvairių subjektų veiklą internete, yra pakankama panaikinti vartotojų nepasitikėjimą. Ar visos priemonės užtikrinti vartotojų duomenų saugumą yra išnaudotos? Jeigu vartotojų pasitikėjimas yra per mažas, galbūt naujoji duomenų apsaugos reforma su BDAR priešakyje yra aiškus ir pakankamas atsakymas į šią problemą? O gal vartotojai patys turi ir gali imtis priemonių savo duomenų apsaugai? Toliau darbe bus bandoma atsakyti į visus šiuos klausimus, aptariant dažniausius asmens duomenų panaudojimo būdus internete bei pasirinktoje srityje analizuojant asmens duomenų rinkimo būdus ir susijusias problemas.

3.1 Vartotojų elgsena grįstos reklamos samprata ir veikimas

Anksčiau aptarta teisės aktuose įtvirtinta duomenų tvarkymo sąvoka apėmė daugybę atskirų veiksmų. Svarbu suprasti, kad visi tie veiksmai elektroninėje erdvėje yra vienas su kitu persidengiantys, dažnai juos nuo kitų skiria itin trumpas laiko tarpas (pavyzdžiui, tam tikrų duomenų automatinį rinkimą, įrašymą, adaptavimą ir analizę internete gali skirti tik kelios milisekundės). Atkreipiamas dėmesys, kad ADTAĮ, 95/46/EB direktyvoje ar BDAR atskiri asmens duomenų rinkimo ir naudojimo apibrėžimai nėra pateikiami. Tai aiškintina tuo, kad šie veiksmai neturi kažkuo išsiskiriančios reikšmės asmens duomenų apsaugos kontekste. Asmens duomenų rinkimas darbe turėtų būti suprantamas kaip

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

asmens duomenų telkimas į vieną vietą, o asmens duomenų naudojimas yra duomenų kaip įrankio vartojimas, siekiant tam tikro tikslo[95].

Asmens duomenis elektroninėje erdvėje įvairioms reikmėms naudoja tiek valstybės institucijos (pvz., baudžiamajame tyrime, žvalgyboje, sveikatos apsaugoje), tiek mokslo įstaigos (pvz., moksliniuose tyrimuose), tiek verslas. Šiame darbe, nagrinėjant asmens duomenų naudojimo klausimą, ir toliau bus koncentruojamasi į verslo subjektų veiklą. Tiksliau dėmesys bus kreipiamas į internetinę reklamą, kurią naudoja verslo subjektai. Tokį pasirinkimą sąlygojo kelios priežastys. Pirma, dauguma verslo subjektų, kurie teikia „nemokamas“ paslaugas internete, yra tiesiogiai priklausomi nuo parduodamos reklamos ar jos vietos kiekio[96]. Antra, didelė dalis verslo subjektų susidomi galimybe savo vartotojus pasiekti pasitelkiant reklamą internete[97]. Taigi internetinė reklama yra net labai paplitusi, o kartais ir gyvybiška, verslo kasdienybės dalis. Reklama internete yra ypač aktuali šio darbo temai, kadangi kai kurių jos rūšių technologinis įgyvendinimas yra pagrįstas surinktų asmens duomenų panaudojimu. Asmens duomenų naudojimas reklamai padeda geriau pažinti interneto vartotojo poreikius ir interesus, o tai padeda verslo subjektams parduoti žymiai daugiau produktų ar paslaugų. Dėl šios priežasties jau dabar asmens duomenys yra vadinami „naująja interneto nafta“ ir „nauja technologinio pasaulio valiuta“[98]. Todėl tik iš pirmo žvilgsnio gali atrodyti, kad dauguma paslaugų internete yra nemokamos. Iš tiesų, vartotojai, naudodamiesi socialiniais tinklais, elektroniniu paštu ar skaitydami naujienas internete, sumoka nustatytą kainą, leisdami suinteresuotiems subjektams neatlygintinai naudotis jų duomenimis[99].

---

[95] Taip pat ši žodžiai „rinkimas“ ir „naudojimas“ aiškinami Dabartinės lietuvių kalbos žodyne. Žr. *Dabartinės lietuvių kalbos žodynas* [interaktyvus]. [žiūrėta 2017 m. vasario 25 d.]. Prieiga per internetą: < http://lkiis.lki.lt/dabartinis >.

[96] Pavyzdžiui, apie 90% visų *Google* turimų įmonių 2015 metais gautų pajamų sudarė pajamos iš reklamos internete. *Facebook* pajamų dalis iš internetinės reklamos tais pačiais metais siekė apie 95%. Žr. Statistikos portalas *Statista* [interaktyvus]. [žiūrėta 2017 m. vasario 25 d.]. Prieiga per internetą: < https://www.statista.com/statistics/266206/googles-annual-global-revenue/ > ir < https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ >.

[97] Oficialiais *Eurostat* duomenimis 2016 metais 1 iš 4 verslo subjektų ES valstybėse narėse naudojosi internetine reklama. Lietuvoje tais pačiais metais tokiomis paslaugomis naudojosi net trečdalis apklausoje dalyvavusių verslo subjektų. Tai reiškia, kad Lietuva šiuo klausimu smarkiai viršija ES vidurkį ir yra penktoje vietoje pagal internetine reklama besinaudojančių verslo subjektų skaičių. Žr. *Eurostat newsrelease*, 2016 m. gruodžio 14 d., Nr. 252/2016. [interaktyvus]. [žiūrėta 2017 m. vasario 25 d.]. Prieiga per internetą: < http://ec.europa.eu/eurostat/documents/2995521/7772211/9-14122016-BP-EN.pdf/74f18ee1-07d3-4617-a33c-c84275ac8aa4 >.

[98] MARKOU, C. Behavioural Advertising and the New ‘EU Cookie Law’ as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 229.

[99] OTT, N., ZYLBERBERG, H. A European Perspective on the Protection of Personal Data in Cyberspace: Explaining How the European Union Is Redefining Ownership and Policies of Personal Data beyond National Borders. *Harvard Kennedy School Review*, 2016, vol. 16, p. 69.

Asmens duomenų rinkimas ir naudojamas elektroninėje erdvėje būtent rinkodaros ir reklamos tikslais per pastaruosius metus tapo neatskiriama naujųjų technologijų ir interneto visuomenės dalis. Šis dėsnis palietė visas industrijos lygius bei rūšis, o tuo pačiu ir interneto vartotojus, kurie vis dažniau tampa internetinio sekimo (angl. *online tracking*) taikiniais. Technologijos, naudojamos interneto vartotojų sekimui Europos Sąjungoje, yra reguliuojamos anksčiau darbe aptartų asmens duomenų apsaugos taisyklių, kadangi šios technologijos dažnu atveju leidžia vartotojus identifikuoti arba potencialiai išskirti iš grupės. Vis dėlto, būdai (technologijos), kuriais yra įgyvendinami rinkodaros tikslai internete, be galimai teigiamų dalykų (aktualios ir pagal interesus pateikiamos reklamos) dažnai sukelia pavojų vartotojų privatumui[100]. Kaip jau buvo minėta, papildomos rizikos, susijusios su technologijų modernėjimu, buvo ir viena iš priežasčių, pradėjusių ES duomenų apsaugos reformą.

Atkreiptinas dėmesys, kad ne visos technologijos, susijusios su internetine reklama, savo reikmėms naudoja asmens duomenis. Pavyzdžiui, vienos iš labiausiai pasaulyje paplitusių – kontekstinės reklamos (angl. *contextual advertising*) – atveju reklama interneto vartotojams rodoma pasitelkiant raktinius žodžius (t. y. kontekstą) lankomame tinklapyje, o ne asmenį galinčius identifikuoti duomenis. Tokiu būdu prie naujienų portale esančio straipsnio, kuriama kalbama apie praėjusios vėtros padarinius, gali būti matoma automobilio ar būsto draudimo reklama. Taip pat internete gali būti naudojama ir statinė reklama, kuri savo principu yra identiška reklamai popierinėje spaudoje (pavyzdžiui, puodų reklama su kulinarija susijusioje laikraščio skiltyje). Tačiau ypatingo privatumo šalininkų dėmesio ir susirūpinimo dėl vartotojų asmens duomenų naudojimo internete susilaukia būtent vartotojų elgsena grįstos reklamos (angl. *behavioural advertising*) metodai. Dėl šios priežasties toliau šiame darbe vartotojų elgsena grįstos reklamos samprata ir metodai bus aptariami plačiau.

Vartotojų elgsena grįsta reklama (toliau ir – VEGR) suprantama kaip „reklama, grindžiama asmenų elgsenos stebėjimu ilgą laiką. Vartotojų elgesiu grindžiama reklama siekiama ištirti šio elgesio savybes remiantis vartotojų veiksmais (kartotiniais apsilankymais svetainėse, sąveikomis, reikšminiais žodžiais, internetinio turinio gamyba ir pan.), kad būtų galima sukurti konkretų profilį ir taip duomenų subjektams pateikti numanomus jų pomėgius atitinkančius konkrečiam asmeniui pritaikytus reklaminius

[100] SKOUMA, G., LÉONARD, L. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Iš *Reforming European Data Protection Law*. S. Gutwirth *et al.* (eds.), Law, Governance and Technology, Vol. 20. Belgium: Springer, 2015, p. 35.

pranešimus“[101]. Elektroninėje erdvėje VEGR yra gana lengvai įgyvendinama bei pagrįsta plačiai paplitusiomis internetą naudojančiomis technologijomis, kurias turi dauguma asmenų (kompiuteris, išmanusis telefonas ir kt.). Dažniausiai įgyvendinant vartotojų elgsena grįstos reklamos metodus dalyvauja trys subjektai – tai reklamuotojai (angl. *advertisers*), kurie pageidauja reklamuoti savo paslaugas ar produktus, interneto svetainių skelbėjai (angl. *publishers*), t. y. interneto tinklalapių savininkai, kurie parduoda vietą kitų subjektų reklamai, ir reklamos skelbimų tinklų operatoriai (angl. *ad network providers*), kurie veikia kaip jungiamoji grandis tarp reklamuotojų ir interneto svetainių skelbėjų[102]. Bendru VEGR atveju, interneto svetainių skelbėjas (šiuo atveju tai gali būti naujienų tinklapis) nustato galimas reklamų vietas savo tinklalapyje ir jas „išnuomoja“ reklamos skelbimų tinklų operatoriui. Reklamuotojas, kuris siekia padidinti savo produkto (sakykime, prabangių kvepalų) žinomumą, kreipiasi į reklamos skelbimų tinklų operatorių ir nurodo, kuriem vartotojų segmentams ar jų grupei turėtų būti rodoma konkretaus produkto reklama. Pavyzdžiui, pasirenkama, jog kvepalų reklamą matytų tik asmenys, gyvenantys Vilniuje ir Kaune, gaunantys vidutines ar aukštas pajamas ir per pastarąją savaitę internete ieškoję dovanų kokia nors proga. Reklamos skelbimų tinklų operatorius savo žinioje turi dideles įvairių vartotojų duomenų bazes, kurios, pasitelkus atitinkamas technologijas, yra panaudojamos atskiriant tam tikrus vartotojų segmentus nuo kitų. Šios technologijos yra susietos su minėtu naujienų tinklalapiu ir tai reiškia, kad konkrečią prabangių kvepalų reklamą matys tik reklamuotojo nurodytų segmentų vartotojai.

Reikia turėti omenyje, kad aukščiau pateiktas pavyzdys aiškumo dėlei yra labai supaprastintas. Iš tiesų reklamos skelbimų tinklų operatorius apjungia daugybę interneto svetainių skelbėjų ir reklamuotojų, todėl dažniausiu atveju reklamuotojas net nežino, kuriame interneto tinklalapyje pasirodys jo reklama[103]. Tačiau jam to žinoti ir nėra būtina, kadangi reklamuotojo tikslas yra toks, kad konkreti reklama pasiektų atitinkamą vartotoją bet kurioje reklamos skelbimų tinklų operatoriaus tinklui priklausančioje interneto svetainėje. Tuo pačiu, interneto svetainių skelbėjai reklamos vietas dažniausiai rezervuoja keliems reklamos skelbimų tinklų operatoriams[104].

---

[101] 29 straipsnio duomenų apsaugos darbo grupės 2010 m. birželio 22 d. priimta „Nuomonė 2/2010 dėl vartotojų elgesiu grindžiamos internetinės reklamos“, 00909/10/LT, WP171, 2010, p. 4.
[102] *Ibid., p. 5.*
[103] *Ibid*.
[104] Kokie reklamos skelbimų tinklų operatoriai bendradarbiauja su atskirais interneto svetainių skelbėjais galima sužinoti nemokamai įsidiegus specialius interneto naršyklės papildinius (pavyzdžiui, *Ghostery*). Apsilankius bet kurioje interneto svetainėje šie naršyklės papildiniai, be kita ko, parodo skirtingų reklamos skelbimų tinklų operatorių, kurie naudoja įvairias vartotojo sekimo technologijas tame puslapyje, pavadinimus.

Taip pat paminėtina, kad vartotojų elgsena grįstos reklamos būdas, kai parenkami atskiri vartotojų segmentai, nėra vienintelis galimas. Praktikoje taikomi ir vartotojų elgesiu pagrįsta pakartotinio nukreipimo paslauga (angl. *behavioural retargeting*). Tai reiškia, kad, kartą apsilankius konkrečiame tinklapyje ir peržiūrėjus atitinkamą prekę, minėta prekė bus rodoma reklamoje kituose po to aplankytuose interneto tinklapiuose (t. y. reklama seks paskui vartotoją)[105]. Be to, naujos technologijos sudaro galimybę vartotojams pateikti reklamas ne tik juos suskirsčius į segmentus, bet ir įvairių algoritmų pagalba (pavyzdžiui, ekstrapoliacijos būdu) bandant nuspėti vartotojų ateities sprendimus (angl. *predictive behavioural targeting*). Taigi, vartotojų elgsena grįstos reklamos tinklas yra didžiulis, o galimybės pasiekti vartotojus, naudojantis jų pačių duomenimis, yra plačios.

3.2 Renkamų ir naudojamų duomenų pobūdis

Natūralu, jog aprašytos sistemos nuolatiniam palaikymui yra būtini pakankamai patikimi duomenys apie interneto vartotojus. Tam, kad interneto vartotojų duomenys būtų laikomi patikimais, būtina juos ne tik tinkamai surinkti, bet ir išanalizuoti. Duomenų rinkimas yra tik pirmas žingsnis visame procese. Surinkti vartotojo duomenys iš įvairių šaltinių yra apjungiami, siekiant atrasti unikalius požymius ir padaryti prasmingas išvadas apie asmenį. Tada turimi duomenys yra lyginami su kitų vartotojų duomenimis, o taip iš identifikuotų skirtumų yra sudaromas atitinkamo vartotojo profilis[106]. Akivaizdu, kad apie atitinkamą asmenį sukauptos žinios nėra nei technologinio, nei empirinio pobūdžio. Asmens sekimas internete sudaro galimybę surinkti daug ir labai įvairių duomenų apie jį, nuo prisijungimo duomenų (pvz., vartotojo vardas) ar tinklo duomenų (pvz., IP adresas) iki informacijos, kuri atskleidžia vartotojo asmenybės bruožus, interesus, pomėgius, įpročius ir pan. Dažnai sukauptos žinios gali atskleisti ir itin jautrią informaciją apie asmenį, pavyzdžiui, jo seksualinę orientaciją ar politinius įsitikinimus[107]. Visi šie surinkti duomenys naudojami siekiant vienokiu ar kitokiu būdu pateikti atitinkamam interneto vartotojui paslaugos ar produkto reklamą.

Vis dėlto, turint omenyje pirmoje ir antroje darbo dalyse analizuotą asmens duomenų sąvoką, gali iškilti klausimas dėl galimybės tokius apie interneto vartotoją

[105] Plačiau pasidomėti galima žiniasklaidos priemonėse, pavyzdžiui žr. *Retargeting Ads Follow Surfers to Other Sites*. New York Times, 2010-08-30. [interaktyvus]. [žiūrėta 2017 m. vasario 28 d.]. Prieiga per internetą: < http://www.nytimes.com/2010/08/30/technology/30adstalk.html >.
[106] SKOUMA, G., LÉONARD, L. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Iš *Reforming European Data Protection Law*. S. Gutwirth *et al.* (eds.), Law, Governance and Technology, Vol. 20. Belgium: Springer, 2015, p. 38.
[107] *Ibid.*, p. 37.

surinktus duomenis vadinti asmens duomenimis. Daugelis vartotojų elgsena grįsta reklama užsiimančių įmonių teigia, kad tol, kol šių įmonių renkami duomenys nėra susieti su konkrečiais vartotojų vardais, galima laikyti, kad jos neužsiima asmens duomenų tvarkymu, todėl asmens duomenų teisinės apsaugos reguliavimas jiems neturėtų būti taikomi[108]. Pagal jau nagrinėtą ES teisinį reguliavimą dėl asmens duomenų sampratos, turėtų būti žinoma, kad asmens duomenimis laikomi ne tik asmenį identifikuojantys duomenys, bet ir jį galimai (potencialiai) identifikuojantys duomenys, priklausantys nuo išteklių ir pastangų, kurias konkrečiu atveju įmanoma skirti. Natūralu, kad ištekliai tarp įvairių verslo subjektų yra pasiskirstę nevienodai. Todėl pasitaiko atvejų, kai atskiros duomenų apsaugos priežiūros institucijos laikosi reliatyvaus požiūrio, jog turimi duomenys yra potencialiai identifikuotini vieniems verslo subjektams, tačiau neidentifikuotini kitiems[109]. Tokiu būdu yra palaikoma ir jau išdėstyta vartotojų elgsena grįsta reklama užsiimančių įmonių pozicija, kad duomenų apsaugos įstatymai tam tikrais atvejais jiems neturėtų būti taikomi.

Visgi, autoriaus nuomone, su tokia pozicija negalima sutikti. Pirmoje darbo dalyje jau buvo užsiminta, kad šiuolaikinės technologijos panaikina ribas tarp asmenį identifikuojančios ir neidentifikuojančios informacijos, suteikdamos sąlygas turimą informaciją gretinti su elektroninėje erdvėje prieinama informacija. Tačiau, kalbant apie vartotojų elgsena grįstą reklamą, identifikuoti asmenį ja užsiimančioms įmonėms gali būti dar paprasčiau (tam pačiam tikslui pasiekti sunaudojama mažiau pastangų ir išteklių).

Pirma, neretai interneto svetainių skelbėjai ir reklamos skelbimų tinklų operatoriai yra tie patys ar susiję asmenys, ypač, kai turima omenyje didžiausius vartotojų sekimo tinklus valdančius verslo subjektus (kaip *Google* ar *Facebook*[110]). Tai reiškia, kad, vartotojui pačiam nurodžius savo asmens duomenis interneto svetainių skelbėjo tinklapyje, nėra technologinio barjero, kuris užkirstų kelią šiuos jau turimus asmens duomenis susieti su vartotojo paspaudimais, atliktais ten, kur tos pačios įmonės veikia kaip tretieji asmenys[111]. Tokiu būdu asmens identifikavimui nėra reikalingi jokie papildomi ištekliai.

---

[108] ZUIDERVEEN BORGESIUS, F. J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(2), p. 256.

[109] *Ibid*., p. 264.

[110] Šiame darbe vartojami pavadinimai *Google, Facebook, Yahoo* ir pan. atskirai turėtų būti suprantami kaip atitinkami verslo subjektai, apimantys visus susijusius juridinius asmenis, neatsižvelgiant į tokių susijusių įmonių grupių struktūrą.

[111] Pavyzdžiui, *Google* dukterinė įmonė *Doubleclick* veikia kaip reklamos skelbimų tinklų operatorius naujienų tinklapyje. Vartotojui naviguojant po šį naujienų tinklapį, slapukų pagalba apie šį vartotoją surenkama tam tikra informacija (ką skaitė, kiek laiko skaitė, ar paspaudė ant reklaminių nuorodų ir pan.). Jeigu vartotojas, neištrynęs slapukų, prisijungs prie bet kurios *Google* teikiamos paslaugos (pavyzdžiui,

Antra, vartotojus identifikuojančią informaciją dažnu atveju reklamos skelbimų tinklų operatoriams nutekina patys interneto svetainių skelbėjai. 2011 metais atlikti tyrimai dėl duomenų nutekėjimo internete[112] nustatė, kad net du trečdaliai ištirtų interneto svetainių tiesiogiai perduoda privačius vartotojų duomenis tretiesiems asmenims. Tokie nutekinti duomenys gali būti vartotojų elektroninio pašto adresai, vartotojo identifikavimo numeris, galimai identifikuojanti demografinė informacija (lytis, pašto kodas, interesai), vartotojo tikras vardas ar slapyvardis. Informacijos nutekėjimas dažniausiai įvyksta netyčia, dėl interneto svetainių skelbėjų neišmanymo ar neatsargumo[113].

Trečia, kai kurios įmonės specializuojasi interneto vartotojų identifikavime. Internete pasitaikančių apklausų, siūlančių laimėti prizus, kurių metu vartotojo prašoma įvesti elektroninio pašto adresą, tikslas yra susieti vartotojų vardus ir elektroninio pašto adresus su duomenimis apie jų elgseną. Jeigu asmeninė informacija yra pateikiama subjektui, kuris tam vartotojui buvo išsiuntęs slapuką, tai minėtas subjektas gali juos (turimą informaciją ir slapuką) apjungti[114]. Po to šia informacija jis gali dalintis su kitais subjektais, atlikdamas slapukų sinchronizavimą (apie jį bus rašoma vėlesniame darbo skyriuje).

Pagaliau, vartotojus identifikuojanti informacija trečiosioms šalims gali būti atskleidžiama atsiradus sisteminėms klaidoms interneto svetainių skelbėjų serveriuose ar įvykus įsilaužimams į jų duomenų bazes[115]. Žinoma, negalima vienprasmiškai teigti, kad

---

elektroninio pašto), *Google* kartu su vartotojo prisijungimo gaus ir informaciją, esančią *Doubleclick* slapuke. Tai reiškia, kad *Google* ir *Doubleclick* neabejotinai žinos, jog būtent šis konkretus asmuo apsilankė konkrečiame naujienų tinklapyje. Daugiau apie slapukų naudojimą VEGR tikslams bus kalbama kitame darbo skyriuje.

[112] KRISHNAMURTHY, B., NARYSHKIN, K., WILLS, C. E. *Privacy leakage vs. Protection measures: the growing disconnect.* Web 2.0 Security and Privacy Workshop, 2011, p. 1 [interaktyvus]. [žiūrėta 2017 m. kovo 1 d.]. Prieiga per internetą: < http://w2spconf.com/2011/papers/privacyVsProtection.pdf >.

[113] Pavyzdžiui, vartotojas savo elektroninį paštą naudoja kaip prisijungimo vardą. Vartotojui prisijungus prie interneto svetainės skelbėjo tinklapio, jo elektroninio pašto adresas matomas URL adrese (sakykime, www.sportastau.lt/wp?/email=jonas.jonaitis@pastas.lt). Tuo metu, kai vartotojas jungiasi prie interneto svetainės skelbėjo tinklapio, reklamos skelbimų tinklų operatorius slapuko pagalba gauna pranešimą, kad šiam vartotojui turi būti rodoma reklama. Kartu pranešime pateikiama nuoroda į interneto svetainės skelbėjo tinklapio adresą (kur turi būti rodoma reklama) su vartotojo elektroninio pašto adresu. Detalesnę informaciją apie galimus vartotojų duomenų nutekėjimo atvejus žr. *Ibid*., p. 3-4.

[114] ZUIDERVEEN BORGESIUS, F. J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(2), p. 264.

[115] Pavyzdžiui, 2016 metų pabaigoje įvykęs įsilaužimas į kompanijos *Yahoo* serverius (daugiau informacijos žr. *Yahoo hack: 1bn accounts compromised by biggest data breach in history*. The Guardian, 2016 m. gruodžio 14 d. [interaktyvus]. [žiūrėta 2017 m. kovo 3 d.]. Prieiga per internetą: < https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached >). Taip pat, 2017 metų vasarį nutekinta informacija iš tokių kompanijų kaip *Uber, Fitbit, OKCupid* (daugiau informacijos žr. FOX-BREWSTER, T. *Google Just Discovered A Massive Web Leak... And You Might Want To Change All Your Passwords*. Forbes, 2017 m. vasario 24 d. [interaktyvus]. [žiūrėta 2017 m. kovo 3 d.]. Prieiga per internetą: https://www.forbes.com/sites/thomasbrewster/2017/02/24/google-just-discovered-a-massive-web-leak-and-you-might-want-to-change-all-your-passwords/#1e6f0c5d3ca3 >).

vartotojų elgsena grįsta reklama užsiimantys asmenys išnaudoja neteisėtai į viešumą patekusią informaciją, tačiau tokios galimybės griežtai atmesti taip pat negalima.

Visi aukščiau nurodyti vartotojų elgsenos ir jų tapatybės susiejimo būdai parodo, kaip lengvai ir su nedideliais ištekliais interneto vartotojai trečiųjų asmenų gali būti identifikuojami. Tiesa, kad pats vartotojų elgsena grįstos reklamos verslo modelis nėra pagrįstas konkrečiomis žiniomis apie interneto vartotojų vardus, pavardes, adresus ir kt. Tačiau, atsižvelgus į įmonių kaupiamų duomenų kiekius, turinį, realias technologines galimybes, galima daryti išvadą, jog vartotojų elgsena grįstos reklamos tikslais renkami duomenys turi būti laikomi asmenį potencialiai identifikuojančiais duomenimis – o kartu ir asmens duomenimis tiek pagal galiojančią 95/46/EB direktyvą, tiek pagal BDAR.

3.3 Vartotojų elgsena grįstos reklamos pavojai ir nauda

Interneto vartotojai gali jaustis nesaugiai, žinodami, kad juos potencialiai identifikuojantys duomenys yra renkami ir naudojami interneto reklamos pasiekiamumui gerinti. Nustačius, kad šioms veikloms Europos Sąjungoje yra taikomos asmens duomenų apsaugos taisyklės, tokio nerimo turėtų kilti mažiau. Itin svarbus aspektas yra tas, jog ES asmens duomenų apsaugos reglamentavimo šiuose santykiuose taikymas reiškia, kad vartotojai turi turėti galimybę pasirinkti dėl savo duomenų rinkimo ir naudojimo VEGR tikslams. Interneto vartotojų pasirinkimas leisti tvarkyti savo duomenis idealioje situacijoje turėtų būti pagrįstas informacija apie tokio tvarkymo galimas pasekmes. Todėl yra tikslinga aptarti vartotojų elgsena grįstos reklamos naudą vartotojams ir jos galimus pavojus.

Literatūroje yra išskiriamos toliau nurodytos pagrindinės rizikos, su kuriomis susiduria interneto vartotojas, kai jo atžvilgiu yra taikoma vartotojų elgsena grįsta reklama. Pirmiausia, tai galimas privačios informacijos atskleidimas tretiesiems asmenims. Šiuo atveju galima kalbėti tiek apie dažnai pasitaikančias asmens duomenų vagystes[116], tiek netyčinį privačios informacijos atskleidimą artimoje aplinkoje. Pastaruoju atveju privatūs duomenys gali būti atskleidžiami paprasčiausiai lankantis įvairiose interneto svetainėse per kito asmens paskyrą ar kompiuterį (taip pat ir kitą įrenginį). Kadangi naudojant vartotojų elgsena grįstą reklamą vartotojui yra rodoma reklama, priklausomai nuo kokias interneto svetaines jis aplankė ar kokias užklausas

[116] Pavyzdžiui, vien šio darbo rašymo laikotarpiu autorius gavo du pranešimus iš skirtingų verslo subjektų apie galimą nelegalų jo privačios informacijos pasisavinimą (angl. *notice of data breach*). 2016 m. gruodžio 15 d. iš kompanijos *Yahoo* dėl pasisavintų paskyros duomenų ir 2017 m. kovo 13 d. iš kompanijos *Paula's Choice Europe B. V.* dėl mėginimo pasisavinti kreditinės kortelės informaciją.

pateikė, tai privačią informaciją gali atskleisti pats reklamos turinys[117]. Pavyzdžiui, nėščios moters, kuri dėl kokių nors priežasčių savo nėštumą slepia nuo artimųjų ar kolegų, kompiuteryje pradeda daugėti su vaikais ir jų prekėmis susijusių reklamų[118]. Antra, vartotojų elgsena grįstos reklamos įgyvendinimui apie asmenis yra surenkama daugybė įvairios informacijos, be kita ko, ir apie jų turtinę padėtį, todėl kyla grėsmė dėl vartotojų diskriminavimo siūlomų produktų kainos ir (ar) kokybės atžvilgiu[119]. Privati informacija gali atskleisti, kiek asmuo yra pasirengęs mokėti už tam tikrą produktą ar paslaugą. Tuo pačiu gali parodyti ir rizikas, susijusias su pirkimu, pavyzdžiui, ar asmuo dažnai vėluoja susimokėti už prekes, ar dažnai jas grąžina pardavėjui. Taigi, vartotojams, kurie paprastai linkę labiau išlaidauti ar dažnai grąžina prekes, internete gali būti taikomos (rodomos) aukštesnės tų pačių prekių kainos. Tuo tarpu vartotojams, kurie turi mažesnes pajamas, gali būti siūlomos prastesnės kokybės prekės ir pan.[120]. Trečia, vartotojų sekimas internete taip pat gali sąlygoti jų elgesio internete pasikeitimus ar turėti įtakos priimamiems sprendimams. Asmuo, žinodamas, kad jo elgesys elektroninėje erdvėje yra nuolat stebimas, gali būti priverstas riboti savo elgesį internete[121]. Pavyzdžiui, nustoti skaityti straipsnius ar knygas jautriomis temomis, vengti domėtis nepopuliariomis prekėmis, paslaugomis. Dėl baimės gauti pasiūlymus aukštesnėmis kainomis, vartotojai gali vengti domėtis prabangos prekėmis internete ir pan. Be to, vartotojų elgesiu grįsta reklama gali daryti įtaką vartotojų užsibrėžtiems tikslams, pavyzdžiui, rūkančiam asmeniui gali būti sunkiau mesti rūkyti, jei jį nuolat persekioja reklamos, siūlančios tabaką ar kitas susijusias prekes[122]. Pagaliau, vartotojų profiliavimas, kurio pagrindu interneto svetainių turinys yra pritaikomas konkrečiam asmeniui gali jį patalpinti į tam

---

[117] MARKOU, C. Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 217.

[118] Atvejai, kai verslo subjektai apie moterų nėštumą sužino anksčiau nei pastarųjų artimieji, yra realiai pasitaikantys. Pavyzdžiui, dėl vieno garsiausių tokių atvejų žr. DUHIGGFEB, C. *How Companies Learn Your Secrets*. New York Times, 2012 m. vasario 16 d. [interaktyvus]. [žiūrėta 2017 m. kovo 5 d.]. Prieiga per internetą: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&pagewanted=all?src=tp >.

[119] European Network and Information Security Agency (ENISA). Privacy considerations of online behavioural tracking, 2012, p. 17.

[120] Pavyzdžiui, JAV kelionių užsakymų internetu agentūra *Orbitz Worldwide Inc.* interneto vartotojams, naršantiems kompanijos *Apple Inc.* produktais, savo lankomiausioje tinklalapio dalyje siūlydavo 20 – 30 % brangesnius viešbučių kambarius, nei kitiems vartotojams. Šaltinis žiniasklaidoje: MATTIOLI, D. *On Orbitz, Mac Users Steered to Pricier Hotels*. The Wall Street Journal, 2012 m. rugpjūčio 23 d. [interaktyvus]. [žiūrėta 2017 m. kovo 8 d.]. Prieiga per internetą: https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 >.

[121] MARKOU, C. Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 219.

[122] *Ibid.*

tikrą „informacijos burbulą“. Pavyzdžiui, naujienų puslapis vartotojui rodys tik tokias naujienas, kuriomis asmuo domėjosi prieš tai. Prekių pardavėjas siūlys tik tokias prekes, kurios atitinka vartotojo pomėgius. Paieškos variklis vartotojui pateiks tik tokius paieškos rezultatus, kurie atitinka buvusias jo užklausas ir paspaudimus. Taip personalizuojant visą interneto turinį iš asmens yra atimama galimybė plėsti savo akiratį, sužinoti apie naujus dalykus[123]. Taigi, visos šios rizikos turėtų būti interneto vartotojų individualiai įvertintos prieš sutinkant dėl jų duomenų tvarkymo.

Paminėtina, kad vartotojų elgsena grįstos reklamos atstovai nesutinka su aukščiau išvardytomis grėsmėmis ir įvardija keletą priežasčių, dėl kurių šis reklamos būdas yra naudingas vartotojams. Pirma, pajamos gaunamos iš vartotojų elgsena grįstos reklamos finansuoja nemokamas paslaugas internete (pavyzdžiui, elektroninis paštas, socialiniai tinklai, paieškų varikliai). Šios lėšos taip pat leidžia verslui vystyti naujas visuomenei naudingas technologijas, pavyzdžiui, *Google*, remdamasi vartotojų paieškų rezultatais, sukūrė programą, galinčią nuspėti ligų plitimą šalyse, kuri gali būti panaudojama epidemijų prevencijai[124]. Antra, vartotojų elgsena grįsta reklama yra naudinga tiek produktų ar paslaugų pardavėjams, tiek interneto vartotojams, kadangi padeda jiems atrasti vieni kitus. Be kita ko, interneto vartotojai, naršydami internete, mato tik jiems aktualią, jų interesus atitinkančią reklamą, todėl išvengia jų nedominančios, nereikalingos informacijos[125]. Trečia, vartotojų elgsena grįsta reklama yra svarbi bendram ekonomikos augimui. Ši technologija padeda prekių ir paslaugų teikėjams lengviau ir pigiau pasiekti vartotoją, parduoti daugiau prekių. Be to, vartotojų elgsena grįsta reklama padeda išsilaikyti rinkoje daugeliui interneto svetainių skelbėjų ir sudaro didžiąją dalį jų pajamų[126]. Visi šie argumentai suponuoja, kad ne tik verslui, bet ir interneto vartotojams VEGR metodai atneša visokeriopą naudą, todėl duomenų subjektams yra naudingiau sutikti su VEGR tikslais atliekamu jų duomenų tvarkymu.

Vis dėlto, darbo autoriaus nuomone, vartotojų elgsena grįstos reklamos atstovų argumentai yra kritikuotini. Dvi iš dažniausiai minimų vartotojų elgsena grįstos reklamos naudų yra paremtos vien ekonomine logika. Tai reiškia, kad nauda ekonomikai ir didesnės verslo subjektų pajamos yra priešpastatomi interneto vartotojų privatumui. Pažymėtina, kad teisingumas ir fundamentalios vertybės bei teisės (pavyzdžiui, teisė į privatumą) neturėtų būti matuojamos vien ekonomine nauda ir efektyvumo lygiu.

[123] European Network and Information Security Agency (ENISA). Privacy considerations of online behavioural tracking, 2012, p. 13.
[124] LENARD, T. M., RUBIN, P. H. In Defense of Data: Information and the Costs of Privacy. *Technology Policy Institute Working Paper, Emory Law and Economics Research Paper*, 2009, No. 9-44, p. 2.
[125] *Ibid.*, p. 2.
[126] *Ibid.*, p. 23.

Teisinėje literatūroje nurodoma, kad asmens privatumo vertė patenka už ekonominio apskaičiavimo ir pelno bei nuostolių analizės ribų, kadangi ji labiau susijusi su požiūriu į visuomenę ir laisvę. Per daug dėmesio skiriant ekonominei naudai galima nepastebėti įvairių privatumo pažeidimų, kuriuos kiekybiškai pamatuoti yra sunku[127]. Be to, nei ekonomikos teorija, nei empiriniai ekonominiai tyrimai dar nedavė galutinio atsakymo į klausimą, ar vartotojų elgsena grįstos reklamos metodai vidutiniškai atneša daugiau ar mažiau socialinės naudos[128]. Taip pat reikia prisiminti, kad vartotojų elgsena grįsta reklama nėra vienintelė reklamos rūšis internete ir ji net nėra labiausiai paplitusi rūšis[129]. Tai reiškia, kad ši reklama ir jos technologija nėra vieninteliai būdai aprūpinti interneto vartotojus nemokamomis paslaugomis. Be to, tai reiškia, kad net ir netaikant vartotojų elgsena grįstos reklamos metodų, interneto svetainių skelbėjai ir reklamos skelbimų tinklų operatoriai neliktų be pajamų ir galėtų tęsti savo veiklą, tik naudodamiesi mažiau vartotojų privatumui grasinančiomis technologijomis.

Likęs argumentas, kuris yra palankus vartotojų elgsena grįstai reklamai, yra susijęs su interneto vartotojų interesų patenkinimu. Viešojoje erdvėje tai yra vienas iš dažniausiai taikomų argumentų – reklamos vartotojams parenkamos pagal jų interesus ir pomėgius, todėl neva vartotojai patiria didelę naudą. Pirmiausia reiktų paminėti, kad vartotojų elgsena pagrįstos reklamos pagrindinis tikslas yra parduoti prekes ar paslaugas interneto vartotojams. Jeigu vartotojų elgsena pagrįstos reklamos metodai nebūtų veiksmingi įgyvendinant šį tikslą, tai jais niekas nesinaudotų, šia reklama užsiimantys verslo subjektai negautų pajamų ir tokios reklamos nebebūtų apskritai. Todėl jau vien kalbine prasme argumentas, jog vartotojų elgsena grįsta reklama yra naudinga vartotojams, nes matoma jų interesus atitinkanti reklama, yra neteisingas. Šios reklamos metodai nėra taikomi altruistiniais tikslais, siekiant sukurti įdomesnį, aktualesnį turinį vartotojams. Kaip jau kalbėta, reklamą užsako produktų ar paslaugų reklamuotojas, jis nurodo vartotojus ar jų grupes, kurios turi matyti konkrečią reklamą. Jeigu reklamuotojas nenorės rodyti savo reklamos kuriai nors specifinei grupei asmenų, tai ji jiems rodoma nebus (nesvarbu, kad toje grupėje asmenų interesai ir pomėgiai iš esmės atitiktų reklamuojamą

[127] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 26.
[128] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 24.
[129] Oficialiais Eurostat duomenimis 2016 metais vartotojų elgsena grįsta reklama naudojosi 27% apklaustų ES verslo subjektų, besireklamuojančių internete, tuo tarpu kontekstine reklama naudojosi net 78% verslo subjektų. Žr. *Eurostat newsrelease*, 2016 m. gruodžio 14 d., Nr. 252/2016. [interaktyvus]. [žiūrėta 2017 m. kovo 7 d.]. Prieiga per internetą: < http://ec.europa.eu/eurostat/documents/2995521/7772211/9-14122016-BP-EN.pdf/74f18ee1-07d3-4617-a33c-c84275ac8aa4 >.

produktą). Todėl tai, kad reklama yra parodoma konkrečiam vartotojui, atitinka reklamuotojo interesus, o ne vartotojo. Faktas, kad reklama vartotojui pasirodo įdomi, aktuali, yra tik reklamuotojo interesų taikymo pasekmė. Galima spėti, kad jeigu verslo subjektai iš tiesų siektų suteikti naudą vartotojams, tai reklama elektroninėje erdvėje būtų minimali arba bent jau būtų mažiau įkyri (pavyzdžiui, neužgožtų skaitomo teksto, neblaškytų dėmesio mirgėjimu ir garsais).

Atkreiptinas dėmesys, kad šiame skyriuje išdėstytos pozicijos buvo analizuojamos preziumuojant, jog interneto vartotojas turi realų pasirinkimą dėl jo duomenų tvarkymo VEGR tikslais. Tai reiškia, kad net preziumuojant, jog vartotojas gali visais atvejais sutikti arba nesutikti su jo asmens duomenų rinkimu, jis vis tiek susiduria su tam tikromis čia aptartomis rizikomis, o jo gaunama nauda yra kelianti abejones. Toliau darbe bus bandoma analizuoti, kiek reali yra prezumcija, kad interneto vartotojui sudaroma galimybė pasirinkti dėl jo duomenų tvarkymo, kai kalbama apie VEGR metodus.

3.4 Duomenų rinkimo technologijos vartotojų elgsena grįstos reklamos kontekste

Šiame skyriuje bus analizuojamas konkrečių technologinių priemonių, renkančių įvairius interneto vartotojų duomenis, vaidmuo vartotojų elgsena grįstos reklamos įgyvendinime. Tokios analizės tikslas yra ne pateikti išsamų visų naudojamų priemonių sąrašą, o atskleisti būdus, kuriais šios technologijos gali sukelti grėsmę asmenų privatumui.

1. <u>Slapukai.</u>

Slapukas yra teksto rinkmena, kurią aplankyti tinklalapiai naršyklės pagalba išsaugo vartotojo įrenginyje. Ši teksto rinkmena savyje saugo informaciją apie interneto vartotojo elgesį. Slapukas taip pat gali pasitarnauti kaip unikalus identifikatorius, susiejantis įrenginį, kuriame išsaugotas slapukas, su vartotojo elgesio duomenimis, saugomais serveriuose[130]. Slapukai gali būti kelių rūšių. Pirmosios šalies slapukais (angl. *first party cookies*) vadinami tokie slapukai, kuriuos išsiunčia ir geba perskaityti tik konkretus tinklalapis, kuriame tuo metu lankosi vartotojas. Pirmosios šalies slapukų naudotojai gali pilnai kontroliuoti, kokia informacija juose yra išsaugoma, ir nustatyti, kaip bus panaudota surinkta informacija. Dažnai pirmosios šalies slapukai savyje talpina informaciją, susijusią su techniniais lankomo tinklalapio nustatymais, kurie padeda užtikrinti vartotojų patogumą (pavyzdžiui, vartotojui vieną kartą nustačius, kad tinklalapis

[130] MARKOU, C. Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 215.

turi būti matomas lietuvių kalba, tinklalapis šią informaciją slapuko pagalba įsimins ir vartotojui nebereikės iš naujo keisti kalbos nustatymų). Trečiosios šalies slapukus (angl. *third party cookies*) savo tinklalapyje patalpina ne pats interneto svetainių skelbėjas, o trečioji šalis, pavyzdžiui, reklamos skelbimų tinklų operatorius. Tokiais atvejais interneto svetainių skelbėjas dažnai net nežino, kokia informacija yra renkama šių slapukų pagalba, o tuo labiau nežino, kur ir kaip ji bus panaudota. Akivaizdu, kad trečiosios šalies slapukai yra susiję su didesne rizika vartotojų privatumui, kadangi šiuo atveju vartotojams yra sudėtinga efektyviai kontroliuoti savo duomenų panaudojimą[131]. Slapukai taip pat gali būti seanso (angl. *session cookies*) arba nuolatiniai (angl. *persistent cookies*). Laikoma, kad seanso slapukai kelia mažesnę grėsmę vartotojų privatumui, kadangi jie automatiškai ištrinami uždarius interneto naršyklę ir renka informaciją apie vartotoją tik, kai jis yra konkrečiame tinklapyje. Priešingai, nuolatiniai slapukai išlieka net uždarius interneto naršyklę ir turėtų būti ištrinami paties vartotojo. Nuolatiniai slapukai pasitelkiami asmenį potencialiai identifikuojančios informacijos rinkimui beveik visuose vartotojo lankomuose tinklalapiuose[132]. Paminėtina, kad vos tik atsiradus slapukams, juos naudojantys subjektai galėdavo perskaityti tik savo išsaugotame slapuke esančią informaciją. Šiuo metu, siekiant ištobulinti vartotojų profilius, yra naudojamas slapukų sinchronizavimas. Jis leidžia atskiriems duomenis renkantiems subjektams susipažinti su kitų subjektų slapukuose saugoma informacija taip išplečiant informacijos tinklą ir palengvinant interneto vartotojo sekimą[133]. Nepaisant slapukų sinchronizacijos, apsilankius bet kurio interneto svetainių skelbėjo puslapyje, vartotojo kompiuteryje bus išsaugomi dešimtys trečiųjų šalių slapukų.

2. <u>Superslapukai ir amžinieji slapukai.</u>

Superslapukais (angl. *super cookies*) vadinami slapukai, kuriuos vartotojui yra labai sudėtinga aptikti ir pašalinti iš turimo įrenginio. Dažniausiai pasitaikanti superslapukų rūšis yra *flash* slapukai. *Flash* slapukai savyje talpina iki 25 kartus daugiau informacijos nei įprasti slapukai. Jie saugomi atskirai nuo įprastų slapukų, todėl vartotojai gali nežinoti, kurias rinkmenas reikia panaikinti iš įrenginio, kad kartu būtų panaikinti ir *flash* slapukai. Jokie veiksmai, atliekami su interneto naršykle (pvz., naršymo istorijos,

[131] SKOUMA, G., LÉONARD, L. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Iš *Reforming European Data Protection Law*. S. Gutwirth et al. (eds.), Law, Governance and Technology, Vol. 20. Belgium: Springer, 2015, p. 40.
[132] *Ibid.*
[133] Atlikti tyrimai parodė, kad *Google* valdomas reklamos skelbimų tinklų operatorus *DoubleClick* savo slapukus sinchronizuoja su daugiau nei 125 atskiromis įmonėmis. Žr. ZUIDERVEEN BORGESIUS, F. J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(2), p. 258.

slapukų, spartinančiosios atmintinės ištrynimas), *flash* slapukų nepanaikins[134]. Be to, buvo nustatyta, kad *flash* slapukai yra naudojami įprastų slapukų, kuriuos vartotojas jau ištrynė, atkūrimui (dėl šios savybės *flash* slapukai literatūroje kartais dar vadinami slapukais-zombiais (angl. *zombie cookies*))[135]. Amžinaisiais slapukais (angl. *evercookies*) vadinami slapukų rinkiniai, kurie išsaugomi skirtingose vartotojo kompiuterio vietose. Kaip ir superslapukų atveju, įprastos procedūros, naudojamos slapukų panaikinimui iš interneto naršyklės, šiuo atveju nėra veiksmingos. Tam, kad amžinieji slapukai būtų panaikinti iš vartotojo įrenginio, reikia būtinai ištrinti juos visus, nes net vienas likęs slapukas sugeba atkurti kitus jau vartotojo ištrintus slapukus[136]. Akivaizdu, kad šių technologijų naudojimas praktikoje pažeidžia vartotojų privatumo reikalavimus, kadangi yra nepaisoma vartotojų teisė atsisakyti trečiųjų šalių slapukų. Dar daugiau, interneto vartotojai nėra atskirai įspėjami apie būtent superslapukų ar amžinųjų slapukų naudojimą ir jiems nesuteikiama galimybė jų atsisakyti. Autoriaus žiniomis, dėl šių technologijų naudojimo kelios bylos buvo pradėtos tik Jungtinėse Amerikos Valstijose[137], tačiau dažniausiai jos baigdavosi taikos sutartimis, pagal kurias atsakovai sumokėdavo atitinkamas kompensacijas ieškovams.

3. Įrenginių identifikavimas.

Įrenginio identifikavimas (angl. *device fingerprint*) suprantamas kaip informacijos elementų rinkinio panaudojimas, siekiant išskirti įrenginį iš kitų, nustatyti įrenginio ryšius su jau turimais duomenimis ar padaryti išvadas apie įrenginio naudotoją[138]. Identifikuojami gali būti daugybė įrenginių, kurie turi prieigą prie interneto (elektroninės knygų skaityklės, išmanieji televizoriai ir pan.), tačiau vienas iš dažniausiai identifikuotinų įrankių yra interneto naršyklė. Interneto naršyklės identifikavimas (angl. *browser fingerprinting*) atliekamas surinkus duomenis apie vartotojo naršyklės

[134] TENE, O., POLONETSKY, J. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology*, 2012, vol. 13, No. 1, p. 288.
[135] TENE, O., POLONETSKY, J. To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology*, 2012, vol. 13, No. 1, p. 289.
[136] SKOUMA, G., LÉONARD, L. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Iš *Reforming European Data Protection Law*. S. Gutwirth et al. (eds.), Law, Governance and Technology, Vol. 20. Belgium: Springer, 2015, p. 42.
[137] Pavyzdžiui, byloje *Del Vecchio et al*. v. *Amazon.com Inc*., Nr. 2:11-cv-00366 (US Court for the Western District of Washington) 2011 m. gruodžio 1 d. buvo priimtas sprendimas atmesti ieškovų reikalavimą dėl neįrodyto žalos dėl slapukų naudojimo patyrimo. Apjungtose bylose *in re: Quantcast Advertising Cookie Litigation*, Nr. 2:10-cv-05484-GW-JCG, *in re: Clearspring Flash Cookie Litigation*, Nr. 2:10-cv-05948-GW-JCG (US District Court Central District of California) 2011 m. birželio 13 d. taikos sutartimi už *flash* slapukų naudojimą atsakovai ieškovams iš viso sumokėjo 2,4 milijono dolerių kompensaciją.
[138] Article 29 Data Protection Working Party. Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting, 14/EN WP 224, 2014, p. 4.

nustatymus (naudojamą šriftą, rezoliuciją, spalvas, įskiepius ir kt.). Kiekvienos atskiro vartotojo naršyklės nustatymai yra tokie skirtingi, kad šių skirtumų visuma sudaro sąlygas identifikuoti vartotoją tokiu pat mastu kaip naudojant slapukus[139]. Tai yra, vartotojui gali būti suteikiamas atskiras numeris ar kitas identifikatorius, su kuriuo susiejama apie vartotoją surinkta informacija. Atskiri surenkamos informacijos apie naršyklę elementai nėra laikomi asmenį identifikuojančiais duomenimis, tačiau duomenų visuma gali kelti grėsmę vartotojų privatumui. Pavyzdžiui, naršyklės identifikatoriaus apjungimas su kompiuterio IP adresu, kaip ir superslapukų atveju, leidžia atkurti vartotojo iš naršyklės kartą jau ištrintus slapukus[140]. Interneto naršyklės identifikavimas dažniausiai atliekamas slaptai, vartotojai apie tai nėra informuojami. Taip pat nėra paprastų būdų, kurie leistų tokį identifikavimą aptikti, panaikinti ar pakeisti jo elementus[141]. Šiuo atveju kai kurių apsauginių bei sekimą blokuojančių programų ar įskiepių įsidiegimas kompiuteryje gali net palengvinti naršyklės susekamumą (naujas papildinys bus traktuojamas kaip dar vienas naršyklės unikalumo kriterijus)[142]. Viena iš naujausių naršyklės identifikavimo atmainų rinkoje – identifikavimas pagal piešinį (angl. *canvas fingerprinting*)[143] – naudoja *Canvas* aplikacijų programavimo sąsajas, kad galėtų išgauti vartotojui nematomą atvaizdą su raidėmis ir simboliais, kuris be vartotojo žinios veiktų kaip ilgalaikis ir unikalus naršyklės identifikatorius[144]. Identifikavimas pagal piešinį veikia panašiu principu kaip ir įprasti naršyklės identifikatoriai, tačiau pasižymi galimybe nustatyti unikalesnius naršyklės požymius, kurie lemia daug tikslesnį naršyklės unikalumą (t. y. daug didesnę

[139] Interneto naršyklės identifikavimo pavyzdys galėtų būti 1 milijono interneto vartotojų išskaidymas į atskiras grupes. Sakykime, kad 60% iš minėto milijono vartotojų naudoja *Google Chrome* naršyklę, o 40% *Mozilla Firefox* naršyklę. Šios dvi vartotojų grupės gali būti skirstomos smulkiau dėl to, kad paminėtos naršyklės turi po kelias versijas ir ne visi vartotojai naudoja naujausias. Po to grupės gali būti dar labiau smulkinamos pagal tokius kriterijus kaip įskiepių skaičius ir rūšys, ekrano rezoliucija, kalbos nustatymai ir pan., kol gaunamas unikalus naršyklės nustatymas, priskirtinas atskiram vartotojui ar jų grupei.

[140] ECKERSLEY, P. How Unique Is Your Web Browser? Electronic Frontier Foundation, 2010, p. 4 [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < https://panopticlick.eff.org/static/browser-uniqueness.pdf >.

[141] Article 29 Data Protection Working Party. Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting, 14/EN, WP 224, 2014, p. 7.

[142] ECKERSLEY, P. How Unique Is Your Web Browser? Electronic Frontier Foundation, 2010, p. 14 [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < https://panopticlick.eff.org/static/browser-uniqueness.pdf >.

[143] Literatūroje ar net žiniasklaidos priemonėse lietuvių kalba tokie vartotojų sekimo metodai kaip *browser fingerprinting* ir *canvas fingerprinting* dar nebuvo aprašyti, todėl nėra oficialių šių metodų pavadinimų vertimų į lietuvių kalbą. Šiame darbe vartojami pavadinimai, atitinkamai naršyklės identifikavimas ir identifikavimas pagal piešinį, yra suteikti autoriaus, atsižvelgiant į sąvokų anglų kalba reikšmę.

[144] ACAR, G., *et al*. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. Study on web tracking mechanisms*. US Princeton University and University of Leuven in Belgium, 2014, p. 674 [žiūrėta 2017 m. kovo 14 d.]. Prieiga per internetą: < https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf >.

galimybę išskirti vartotoją iš grupės)[145]. Be to, jeigu vartotojas, įdėjęs laiko ir pastangų, įprastus naršyklės identifikatorius gali užblokuoti, tai rinkoje šiuo metu nėra būdo, kuris užblokuotų identifikavimą pagal piešinį, nepažeidęs lankomų tinklapių funkcionalumo[146]. Dėl ribotos darbo apimties kiti rinkoje egzistuojantys įrenginių identifikavimo metodai toliau aptariami nebus[147], tačiau galima teigti, kad tie metodai, kurie buvo aptarti, atskleidė šių technologijų pagrindinius principus ir vartotojų privatumui keliamas grėsmes.

4. *Socialiniai tinklai ir vartotojų stebėsena.*

Vartotojų stebėsena socialiniuose tinkluose nėra susieta su kokia nors ypatinga technologija. Socialiniai tinklai tiesiog stebi vartotojų elgesį jų platformose (t. y. jų paspaudimus, pasidalinimus, laiką, praleistą prie vieno ar kito užsiėmimo). Dažniausiai socialinių tinklų vartotojai patys mielai dalinasi savo ir savo šeimos asmeninio gyvenimo detalėmis. Socialiniai tinklai visą apie vartotojus surinktą informaciją panaudoja platformų tobulinimui ir reklamų pritaikymui pagal vartotojų interesus (arba tiksliau reklamų rodymu tiems vartotojams, kurių pageidauja reklamuotojai). Pažymėtina, kad duomenys apie socialinių tinklų vartotoją gali būti renkami jam net nesant pačioje socialinio tinklo platformoje. Pavyzdžiui, tuo atveju, jei kokia nors interneto svetainė prie pateikiamo teksto turi integruotą *Facebook* mygtuką „patinka“, vien tokio mygtuko buvimas tinklapyje reiškia, kad vartotojo elgesys yra sekamas, vartotojui net nebūtina šio mygtuko paspausti[148]. Duomenys renkami netgi tuo atveju, jei vartotojas prieš tai buvo nusprendęs nepriimti *Facebook* siunčiamų slapukų ar apskritai nebuvo *Facebook* socialinio tinklo naudotojas[149]. Toks pat interneto vartotojų sekimo principas yra taikomas ir kitų socialinių tinklų platformų atveju.

---

[145] Informacija apie šį interneto vartotojų sekimo metodą buvo pasirodžiusi ir žiniasklaidoje, pavyzdžiui žr. *Browser 'fingerprints' help track users*. BBC News, 2014 m. liepos 22 d. [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: http://www.bbc.com/news/technology-28423257 >.

[146] ACAR, G., et al. *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. Study on web tracking mechanisms*. US Princeton University and University of Leuven in Belgium, 2014, p. 674 [žiūrėta 2017 m. kovo 14 d.]. Prieiga per internetą: < https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf >.

[147] Plačiau apie taikomas technologijas įrenginių identifikavimo sferoje bei jų paplitimą žr. ENGLEHARDT, S., NARAYANAN, A. Online Tracking: A 1-million-site Measurement and Analysis. Paper of US Princeton University, 2016, p. 11-14 [interaktyvus]. [žiūrėta 2017 m. kovo 15 d.]. Prieiga per internetą: < http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf >.

[148] European Network and Information Security Agency (ENISA). Privacy considerations of online behavioural tracking, 2012, p. 9.

[149] Dėl tokio *Facebook* elgesio Belgijos duomenų apsaugos priežiūros institucija kreipėsi į Belgijos teismus. Pirma teismo instancija nurodė socialiniam tinklui sustabdyti vykdomą interneto vartotojų sekimą be jų sutikimo. Apeliacinė instancija panaikino pirmosios instancijos teismo sprendimą tuo pagrindu, kad Belgijos duomenų apsaugos priežiūros institucija neturėjo įgaliojimų kreiptis į teismą Belgijoje dėl

3.5 Teisės įgyvendinimo problemos verslo subjektų praktikoje

Visus arba daugumą aukščiau aprašytų technologijų vienija tam tikra tendencija – vartotojas nėra informuojamas apie aprašytų metodų naudojimą, jam neleidžiama nesutikti su duomenų rinkimu, o jeigu vartotojas išreiškia nesutikimą, į jį nekreipiama dėmesio. Be to, interneto vartotojas susiduria su apsunkintomis sąlygomis, jeigu jis pageidauja nutraukti vykdomą sekimą ir ištrinti kompiuteryje ar naršyklėje saugomas rinkmenas, trečiųjų asmenų naudojamas jo duomenų rinkimui. Akivaizdu, kad toks elgesys neatitinka šiuo metu galiojančioje 95/46/EB direktyvoje iškeltų reikalavimų asmens duomenų tvarkymui. Konkrečiai prieštarauja 10, 11 ir 14 straipsniuose įtvirtintoms nuostatoms dėl prievolės informuoti duomenų subjektą, kai jo duomenys renkami, taip pat dėl duomenų subjekto teisės prieštarauti duomenų apie jį tvarkymui[150]. Atkreiptinas dėmesys, kad šiuo metu asmens duomenų tvarkymą elektroninėje erdvėje reglamentuoja ne vien jau darbe aptarti teisės aktai, bet ir vadinamasis „ES slapukų įstatymas“ (angl. *EU cookie law*)[151]. 2009/136/EB direktyvos, kurioje įtvirtinti direktyvos 2002/58/EB dėl privatumo ir elektroninių ryšių pakeitimai, 5 straipsnio 3 dalyje nustatyta, kad valstybės narės privalo užtikrinti, jog saugoti informaciją arba suteikti galimybę naudotis jau saugoma informacija naudotojo galiniame įrenginyje būtų leidžiama tik su sąlyga, kad naudotojas davė savo sutikimą. Toje pačioje dalyje įtvirtinta, kad sutikimas turi būti duotas naudotojui pateikus aiškią ir išsamią informaciją pagal 95/46/EB direktyvos reikalavimus. Taigi, pagal šią nuostatą interneto svetainės turėtų nenaudoti slapukų, nebent būtų gautas informuotas interneto vartotojo sutikimas.

Vartotojo sutikimui taikomi visi anksčiau skyriuje dėl duomenų tvarkymo aptarti reikalavimai. Nagrinėjama nuostata numato tik dvi galimas išimtis iš taisyklės: 1) kai naudojant slapuką siekiama tik atlikti pranešimo perdavimą elektroninių ryšių tinklu; 2) kai slapukas naudojamas būtinais atvejais, kad informacinės visuomenės paslaugų

Facebook vykdomų veiksmų, kadangi Facebook padalinys yra įsteigtas Airijoje. Plačiau apie bylą žr. žiniasklaidos priemonėse, pavyzdžiui : WAKEFIELD, J. *What is Facebook doing with my data?* BBC News, 2015 m. lapkričio 10 d. [interaktyvus]. [žiūrėta 2017 m. kovo 14 d.]. Prieiga per internetą: < http://www.bbc.com/news/magazine-34776191 >; taip pat FIORETTI, J. *Facebook wins privacy case against Belgian data protection authority*. Reuters, 2016 m. birželio 29 d. [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV >.

[150] Šių straipsnių atitikmenys Lietuvos nacionalinėje teisėje ADTAĮ 23, 24 ir 27 straipsniai.

[151] 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos Direktyva 2009/136/EB iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo (toliau – 2009/136/EB direktyva). Pažymėtina, kad „ES slapukų įstatymų“ dažniausiai vadinama 2009/136/EB direktyva buvo pakeista 2002/58/EB direktyvos 5 str. 3 dalis, kuri Lietuvos nacionalinėje teisėje yra perkelta į Lietuvos Respublikos elektroninių ryšių įstatymo (su pakeitimais ir papildymais) 61 straipsnio 4 dalį.

teikėjas galėtų teikti paslaugas, kurių aiškiai paprašo naudotojas. Darbo grupė, komentuodama šias išimtis nuomonėje 4/2012[152], paaiškino, kad tiems slapukams, kurie yra būtini operacijoms, vykstančioms internete (dažniausiai tai seanso slapukai), gali būti netaikomas reikalavimas gauti interneto vartotojo sutikimą. Darbo grupė taip pat pateikė tokių išimtinių slapukų pavyzdžius (tapatumo nustatymo, multimedijų grotuvų seanso slapukai ir pan.). Nuomonėje taip pat buvo aiškiai nurodyta, kad interneto vartotojų sekimo ar vartotojų elgsena grįstai reklamai naudojami slapukai nepatenka į išimtį, todėl jų naudojimui yra būtinas vartotojo sutikimas. Metais anksčiau išleistoje Darbo grupės nuomonėje 16/2011[153] akcentuojami praktiniai reikalavimo gauti vartotojo sutikimą įgyvendinimo aspektai. Tai „interneto svetainės viršuje esantis statiškas informacinis langas, kuriame vartotojo prašoma duoti sutikimą naudoti kai kuriuos slapukus“, „iškylantieji langai patekus į interneto svetainę, kuriuose paaiškinama, kokie slapukai bus naudojami ir kokios šalys juos naudos vartotojui sutikus“, „numatytosios nuostatos, kuriomis draudžiama perduoti duomenis išorės šalims ir reikalaujama, kad vartotojas paspaustų nuorodą ir taip išreikštų savo sutikimą būti stebimam“ ir „numatytieji naršyklių nustatymai, kurie padėtų užtikrinti, kad duomenys apie elgesį nebebūtų renkami“[154]. Visi išvardinti būdai yra susiję su aktyviu vartotoju dalyvavimu, ypač atsakant dėl galimo slapukų naudojimo vartotojo atžvilgiu. Darbo grupė pabrėžia, jog informacija vartotojui turėtų būti pateikta tiesiogiai (interaktyviai) ekrane, prireikus ir lygmeniniais pranešimais, nurodant subjektus, kurie siunčia slapukus, sekančius vartotojų elgesį jiems naršant internete. Labai svarbu tai, kad Darbo grupė savo nuomonėje 9/2014[155] atkreipė dėmesį į besivystančias interneto vartotojų sekimo technologijas ir nurodė, jog vadinamasis „ES slapukų įstatymas“ turėtų būti taikomas ir įrenginių identifikavimo atvejais. Taigi, visų paminėtų reikalavimų turi būti laikomasi ir naršyklės identifikavimo bei identifikavimo pagal piešinį atvejais.

Vis dėlto, verslo subjektai, nors ir turėdami vadovautis ES oficialiais ir ne oficialiais teisės aktais (nuomonėmis), vietoje to, kad drastiškai pakeistų savo požiūrį į interneto vartotojų sutikimo gavimo procedūrą, ėmėsi vengti nustatytų taisyklių. Jau buvo kalbėta apie atvejus, kai įvairias interneto vartotojų sekimo technologijas naudojantys subjektai tiesiog piktybiškai nepraneša apie šias technologijas vartotojams ir naudoja jas

[152] 29 straipsnio duomenų apsaugos darbo grupės 2012 m. birželio 7 d. priimta „Nuomonė 4/2012 dėl slapukams taikomo reikalavimo gauti sutikimą išimties“, 00879/12/LT, WP 194, 2012.
[153] 29 straipsnio duomenų apsaugos darbo grupės 2011 m. gruodžio 8 d. priimta „Nuomonė 16/2011 dėl EASA / IAB vartotojų elgesiu grindžiamos internetinės reklamos geriausios patirties rekomendacijų“, 02005/11/LT, WP 188, 2011.
[154] *Ibid.*, p. 10 – 11.
[155] Article 29 Data Protection Working Party. Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting, 14/EN, WP 224, 2014.

be vartotojų sutikimo. Dažniausiai pasitaikantys atvejai gal ir nėra tokie drastiški, tačiau piktnaudžiavimo ir siekimo išvengti nustatytų pareigų požymių pasitaiko ir kitokiame verslo subjektų elgesyje. Pavyzdžiui, verslo subjektai vietoje to, kad įgyvendintų interneto vartotojų dalyvavimo modelį (angl. *opt-in*), kaip jis įtvirtintas 2009/136/EB direktyvos 5 str. 3 dalyje, pasirenka įgyvendinti atsisakymo modelį (angl. *opt-out*), kuris buvo įtvirtintas senesnėje direktyvos redakcijoje (direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje)[156].

Siekiant išanalizuoti verslo subjektų požiūrį į 95/46/EB direktyvos ir „ES slapukų įstatymo“ nuostatas Lietuvoje, darbo autorius atliko tyrimą su trimis lankomiausiais lietuviškais naujienų tinklapiais (tyrimo eiga pateikiama darbo priede). Atlikto tyrimo rezultatai patvirtina, kad visos jame dalyvavusios interneto svetainės nesilaiko teisės aktų reikalavimų gauti vartotojų sutikimą prieš išsaugant informaciją (slapukus) vartotojo naršyklėje. Rezultatai, atliekami oficialios duomenų apsaugos priežiūros institucijos Lietuvoje, yra ne ką geresni. Valstybinė duomenų apsaugos inspekcija savo interneto tinklalapyje pateikia įvairiose srityse atliktų patikrinimų rezultatų apibendrinimus nuo 2010 metų. Viename iš savo naujausių apibendrinimų[157] Valstybinė duomenų apsaugos inspekcija nurodo, kad iš 42 patikrinime dalyvavusių bendrovių, kurios tvarko asmens duomenis automatiniu būdu, visose nustatyta ADTAĮ įstatymo pažeidimų, o 37 bendrovėse rasta Lietuvos Respublikos elektroninių ryšių įstatymo pažeidimų. Nustatyta, kad iš pastarųjų 37 bendrovių 33 bendrovės interneto svetainėse nepateikia informacijos apie naudojamus slapukus bei jų įrašymo tikslus, o 25 bendrovėse nėra gaunamas savanoriškas vartotojo sutikimas dėl tokios informacijos įrašymo į vartotojo galinį įrenginį. Apibendrinimo pabaigoje nurodoma, kad visoms tikrintoms bendrovėms pateikti nurodymai pašalinti nustatytus pažeidimus. Palyginimui, 2012 metais atliktame patikrinime[158] nustatyta, kad, patikrinus 23 bendroves, 22 iš jų nebuvo pateikta informacija apie konkrečiose interneto svetainėse naudojamus slapukus bei jų įrašymo tikslus, taip pat nebuvo gaunamas vartotojo sutikimas dėl slapukų įrašymo. Apibendrinimo pabaigoje taip pat nurodoma, kad visoms tikrintoms bendrovėms pateikti

[156] MARKOU, C. Behavioural Advertising and the New ‘EU Cookie Law’ as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 225.

[157] Valstybinė duomenų apsaugos inspekcija. Paslaugų teikėjų, registruotų valstybinės mokesčių inspekcijos Moss sistemoje, asmens duomenų tvarkymo teisėtumo tikrinimų rezultatų apibendrinimas, 2016 m. gruodžio 29 d.

[158] Valstybinė duomenų apsaugos inspekcija. Internetinių parduotuvių tikrinimų dėl duomenų subjektų teisių įgyvendinimo, asmens duomenų saugojimo teisėtumo ir informacijos saugojimo kliento galiniame įrenginyje ir/ar galimybės naudotis jau saugoma informacija suteikimo teisėtumo rezultatų apibendrinimas, 2012 m. gruodžio 19 d., Nr. 4R-300(17).

nurodymai pašalinti nustatytus pažeidimus. Taigi, palyginus 2012 ir 2016 metų rezultatus, atrodo, kad verslo subjektų daromų pažeidimų mastas iš esmės nesikeičia, net labai didelė dalis institucijos tikrinamų bendrovių nesilaiko teisės aktų nuostatų. Deja, Valstybinė duomenų apsaugos inspekcija nepateikia duomenų, ar pažeidimus padariusiose bendrovėse vėliau atliekami pakartotiniai patikrinimai, todėl negalima patikrinti, kiek pažeidėjų vėliau pakeičia savo elgesį, jei pakeičia.

Tiesa, iš literatūroje pateikiamų pavyzdžių matyti, kad verslo praktika, kai į asmens duomenų apsaugos reikalavimus žiūrima „pro pirštus“, yra paplitusi ir kitose ES valstybėse[159]. Kai kurie autoriai nurodo, jog tokių verslo subjektų daromų pažeidimų priežastys gali būti kelios. Tai vieningas verslo pasipriešinimas vartotojų dalyvavimo modeliui (angl. *opt-in*), to sąlygotas priešiškumas viešojoje erdvėje (neigiamai paveikęs ir pačių interneto vartotojų nuomones) ir neveiksnumas bei nepasirengimas šiai taisyklei tiek ES, tiek nacionaliniu lygmeniu[160].

3.6 Priemonių situacijos gerinimui analizė

Nauji pokyčiai, pirmiausia susiję su BDAR įsigaliojimu, tikėtina paskatins verslo atstovus laikytis teisės aktuose numatytų reikalavimų. Tačiau taip pat paminėtina, kad 2017 m. sausio 10 d. Europos Komisija pateikė pasiūlymą dėl 2002/58/EB direktyvos panaikinimo ir jos reguliavimo perkėlimo į reglamentą (toliau – Privatumo reglamentas)[161]. Europos Komisijos pasiūlyme yra pripažįstama, kad galinių įrenginių konfidencialumui užtikrinti skirtos sutikimo taisyklės tikslai nėra pasiekti. Nurodoma, kad „galutiniams paslaugų gavėjams tenka atsakyti į prašymus leisti naudoti ilgalaikius slapukus, nors jie ir nesupranta tokių slapukų prasmės, o kai kuriais atvejais slapukai išsaugomi netgi be jų sutikimo. Sutikimo taisyklės taikymo sritis yra pernelyg plati, nes ta taisyklė taikoma ir veiklai, kuri nedaro poveikio privatumui, ir kartu per siaura, nes į jos taikymo sritį nėra aiškiai įtrauktos tam tikrų rūšių sekimo priemonės (pavyzdžiui, įrenginių identifikavimas), kurios nebūtinai turi būti susijusios su prieiga prie duomenų arba jų saugojimu įrenginyje“[162]. Pasiūlyto naujo Privatumo reglamento nuostatose atsispindi griežta Europos Komisijos pozicija dėl interneto vartotojų sekimui taikomų technologijų naudojimo. Pirmiausia, Privatumo reglamento

[159] MARKOU, C. Behavioural Advertising and the New ‘EU Cookie Law’ as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 225-226.
[160] *Ibid.*, p. 238 – 239
[161] Europos Komisija. Pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių). Briuselis, 2017 m. sausio 10 d.
[162] *Ibid.*, p. 6.

konstatuojamosios dalies 20 punkte yra aiškiai įvardijama, kad metodai, kuriais slapta stebimi galutinių paslaugų gavėjų veiksmai (pvz., sekama jų veikla internete), kelia didelę grėsmę vartotojų privatumui[163]. Antra, Privatumo reglamento 8 straipsnio 1 dalyje aiškiai nurodoma, kad į šio reglamento reguliavimo sferą patenka ne tik slapukai, bet ir tokios interneto vartotojų sekimo technologijos kaip įrenginių identifikavimas. Trečia, nurodomas baigtinis sąrašas atvejų, kai informacijos saugojimas ir naudojimas galiniuose vartotojų įrenginiuose yra leidžiamas – tai būtinumas operacijų atlikimui ar paslaugų suteikimui, vartotojo duotas sutikimas ar būtinumas interneto svetainės lankomumui apskaičiuoti. Vartotojui turėtų būti suteikta galimybė išreikšti sutikimą naudojant tinkamus naršyklės ar kitos taikomosios programos nustatymus. Taip pat numatyti reikalavimai, renkant informaciją iš galutinių įrenginių, vartotojui pateikti aiškų pranešimą, nurodantį bent informacijos rinkimo sąlygas, informacijos rinkimo tikslą, už tai atsakingą asmenį ir kitą pagal BDAR nuostatas būtiną pateikti informaciją. Ketvirta, labai svarbu, kad Europos Komisija pripažįsta, jog sutikimas tvarkyti duomenis, gautus naudojant internetą, nebus laikomas galiojančiu, jei duomenų subjektas faktiškai neturės laisvo pasirinkimo arba negalės atsisakyti duoti sutikimą ar sutikimo atšaukti, nepatirdamas žalos. Tai reiškia, kad interneto vartotojui planuojama suteikti niekieno neribojamą teisę pasirinkti dėl jo asmens duomenų naudojimo. Įvertinus šiuos ir kitus smulkiau neaptartus pasikeitimus, galima teigti, kad Europos Komisijos pasiūlymas dėl Privatumo reglamento yra antras tvirtas žingsnis link asmens duomenų judėjimo kontrolės grąžinimo interneto vartotojams Europos Sąjungoje. Lieka tik tikėtis, kad po laukiančio derybų laikotarpio Privatumo reglamento tekstas nepasikeis į blogąją pusę.

Asmens duomenų apsaugą reguliuojančių teisės aktų reforma yra aiškus ženklas subjektams, užsiimantiems interneto vartotojų sekimu tiek vartotojų elgsena grįstos reklamos, tiek kitais tikslais. Reikalavimai, anksčiau buvę įtvirtinti neprivalomuose (angl. *soft law*) teisės šaltiniuose, po reformų įgyvendinimo bus privalomi visiems ES asmens duomenų valdytojams ir tvarkytojams be išimties. Taip pat valstybių narių institucijoms bus suteikti svertai, pagaliau leidžiantys taikyti adekvačias poveikio priemones taisyklių nesilaikantiems verslo subjektams. Konkrečiai, tiek BDAR, tiek pasiūlyme dėl Privatumo reglamento valstybių narių priežiūros institucijoms suteikiamos galios skirti administracines baudas net iki 20.000.000 EUR arba įmonės atveju – iki 4 % jos ankstesnių finansinių metų bendros metinės pasaulinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė[164]. Palyginimui, Lietuvoje šiuo metu pagal Lietuvos Respublikos

[163] Europos Komisija. Pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių). Briuselis, 2017 m. sausio 10 d., p. 18.
[164] BDAR 83 str. 5 dalis, Privatumo reglamento 23 str. 3 ir 5 d.

administracinių nusižengimų kodekso 82 straipsnį maksimali bauda už ADTAĮ straipsnių pažeidimą yra 1150 EUR, už pakartotinį nusižengimą – 3000 EUR.

Svarbu, kad nauji svertai įpareigotų nacionalines institucijas skirti daugiau dėmesio asmens duomenų apsaugai elektroninėje erdvėje. Darbo autoriaus vertinimu, šiuo metu Valstybinės duomenų apsaugos inspekcijos prevencinė veikla dėl asmens duomenų rinkimo ir naudojimo elektroninėje erdvėje vykdoma pasyviai bei vadovaujantis neracionaliais metodais[165]. Kadangi technologijos, skirtos asmens duomenų rinkimui ir naudojimui nuolat tobulėja, natūralu, kad naujųjų technologijų įtraukimas į nacionalinės priežiūros institucijų atliekamą prevencinę veiklą taip pat yra būtinas. Jeigu prevencinis verslo subjektų tikrinimas vyktų ten, kur ir yra daromi pažeidimai, t. y. ir elektroninėje erdvėje (o ne vien susirašinėjimo ar fizinio nuvykimo į vietą būdais[166]), būtų pasiekiami net keli pozityvūs rezultatai. Pirma, atliekami patikrinimai būtų informatyvesni, kadangi būtų galima pažeidimus aptikti realiu metu ir pritaikytų technologijų pagalba tiksliai nustatyti pažeidimų pobūdį. Antra, inspekcijos vykdomi patikrinimai elektroninėje erdvėje sumažintų verslo subjektams tenkančią naštą, t. y. sumažėtų jų pildomų dokumentų apimtis. Trečia, naujų technologijų inkorporavimas į atliekamus patikrinimus galėtų leisti padidinti tikrinamų subjektų skaičių, o tai sąlygotų kokybiškesnę kontrolę. Be abejo, reikia pripažinti, kad tinkamai asmens duomenų apsaugos kontrolei įgyvendinti svarbūs ne tik priežiūros institucijų taikomi metodai, bet ir institucijų turimi resursai ir santykis su kitomis valstybės institucijomis. Europos Sąjungoje vis dar pasitaiko atvejų, kai nacionalinė duomenų apsaugos priežiūros institucija kenčia nuo finansinių suvaržymų ar valdžios ir industrijos šališkumo[167]. Taigi, nacionalinėms priežiūros institucijoms būtinas modernus požiūris į internete asmens duomenų apsaugos srityje kylančias problemas ir finansinis bei politinis palaikymas.

---

[165] Pavyzdžiui, Valstybinės duomenų apsaugos inspekcijos 2017 metų prevencinių tikrinimų plane, kuriame nurodomi visi patikrinimai, planuojami tais metais, iš 80 tikrintinų juridinių asmenų tik 5 bus tikrinami dėl atitikimo LR elektroninių ryšių įstatymo 61 str. 4 daliai. Nurodyta, kad šie asmenys bus tikrinami tik susirašinėjimo būdu. Tai reiškia, kad Valstybinės duomenų apsaugos inspekcija realiai netikrina subjektų valdomų interneto svetainių, nenustatinėja, kokie tiksliai duomenys ir kokiais būdais iš vartotojų yra renkami, ar vartotojai realiai yra informuojami apie jų duomenų rinkimą ir pan. Turint omenyje, kad tikrinamos veiklos yra vykdomos internete, natūralu, kad pats tikrinimas taip pat turėtų vykti elektroninėje erdvėje, aplankant interneto svetaines ir įvairių technologijų pagalba nustatant pažeidimus asmens duomenų apsaugos srityje. Taip pat, atsižvelgiant į rinkoje daromų pažeidimų mastą, pasirinktas tikrinamų subjektų skaičius visiems 2017 metams yra aiškiai per mažas. Žr. Valstybinės duomenų inspekcijos direktoriaus 2017 m. vasario 6 d. įsakymu Nr. 3R-60 patvirtintą 2017 m. prevencinių tikrinimų planą [interaktyvus]. [žiūrėta 2017 m. kovo 16 d.]. Prieiga per internetą: < https://www.ada.lt/go.php/lit/Prevenciniai-patikrinimai/2 >.

[166] Tai yra vieninteliai prevenciniai patikrinimo būdai, numatyti Valstybinės duomenų apsaugos inspekcijos prevenciniuose tikrinimo planuose 2014 –2017 metais.

[167] Pavyzdžiui, 2014 metais Teisingumo Teismas sprendė, kad staigus Vengrijos duomenų apsaugos komisaro nušalinimas iš pareigų buvo įvykdytas pažeidžiant Vengrijos duomenų apsaugos institucijos nepriklausomumą ir kartu ES teisę. Europos Sąjungos Teisingumo Teismas. 2014 m. balandžio 8 d. sprendimas *Commission v Hungary* Nr. C-288/12, ECLI:EU:C:2014:237

4. SUBJEKTŲ ATSAKOMYBĖS DĖL ASMENS DUOMENŲ RINKIMO IR NAUDOJIMO PAŽEIDIMŲ PASKIRSTYMO PROBLEMOS

4.1 Asmens duomenų savisauga ir su tuo susijusios problemos

Sąvoka asmens duomenų savisauga (angl. *do-it-yourself (DIY) data protection* arba *self-data-protection*) apima visas priemones, kurių imasi individualus asmuo, siekdamas apsaugoti savo duomenis[168]. Tai gali būti duomenų šifravimas, anonimizavimas, naršyklės įskiepių, kurie kontroliuoja slapukus ar trukdo kitoms sekimo technologijoms, įsidiegimas. Sąvoka apima vartotojų naudojamas duomenų mažinimo strategijas, pavyzdžiui, netikrų duomenų ar profilių naudojimą, duomenų pateikimą tik išimtiniais atvejais bei patikimiems valdytojams ir net tam tikrų technologijų ar paslaugų atsisakymą tuo tikslu. Taip pat tam tikrų teisinių veiksmų taikymą, pavyzdžiui, prašymas verslo subjektui ištrinti visus apie vartotoją surinktus duomenis[169]. Taikydamas asmens duomenų savisaugos priemones, interneto vartotojas gali jausti didesnę savo asmens duomenų kontrolę, todėl šios priemonės dažnai įvardijamos kaip viena iš būtinų visapusiškos duomenų apsaugos dalių[170]. Tačiau galimybės užsiimti savisauga egzistavimas dažnai panaudojamas ir vartotojų elgsena grįstos reklamos gynėjų argumentuose. Būtent, nurodoma, jog interneto vartotojai turi priemones, kurių pagalba gali atsisakyti suteikti savo asmens duomenis verslo subjektams. Šių priemonių nenaudojimas vertinamas kaip pasirinkimas nesidomėti savo asmens duomenų rinkimu ir jų tolesniu likimu bei kaip sąmoningas privatumo atsisakymas[171]. Ir iš tiesų, įvairiose apklausose dauguma interneto vartotojų deklaruoja, jog privatumas jiems yra labai svarbus, bet tie patys asmenys dažnai atskleidžia savo asmens duomenis, gaudami tik minimalią naudą, ir retas imasi technologinių priemonių savo privatumo užtikrinimui[172]. Tokia situacija literatūroje vadinama privatumo paradoksu. Vis dėlto, šiam interneto vartotojų elgesiui paaiškinti galima rasti daug priežasčių, todėl minėti argumentai dėl sąmoningo privatumo atsisakymo turėtų būti vertinami kritiškai.

---

[168] MATZNER, T., *et al*. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 278.

[169] *Ibid.*

[170] European Network and Information Security Agency (ENISA). Privacy considerations of online behavioural tracking, 2012, p. 15.

[171] VAN WELL, L., ROYAKKERS, L. Ethical Issues in Web Data Mining. *Ethics and Information Technology*, 2004, vol. 6, issue 2, p. 135.

[172] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 43.

Pirmiausia, spartus technologijų modernėjimas sąlygoja tai, kad vidutiniam vartotojui yra sudėtinga perprasti technologijas slypinčias už interneto informacijos srautų. Taigi, duomenų apsauga taip pat darosi vis sudėtingesnė. Nors egzistuoja nemažai įrankių, galinčių vienaip ar kitaip padėti apsaugoti vartotojo privačius duomenis, nėra vienos duomenų strategijos ir vieno įrankio, kuris panaikintų visas asmenų privatumui kylančias rizikas. Tam, kad vartotojas suspėtų su technologijų ir duomenų apsaugos strategijų kaita, reikalingas laikas ir specifinės žinios[173]. Dėl šios priežasties asmens duomenų savisauga gali tapti ir tampa privilegija tų, kurie turi laiko ir gali skirti papildomas pastangas susipažinimui su naujomis technologijomis. Teisinėje literatūroje apžvelgiami tyrimai patvirtina, kad daugelis interneto vartotojų nesinaudoja asmens duomenų savisaugos priemonėmis, nes jiems jos per daug sudėtingos[174]. Įvairios interneto vartotojų apklausos[175] atskleidžia dar svarbesnę informaciją – didelė dalis internetą naudojančių asmenų apskritai nežino, kad jų duomenys internete yra renkami vartotojų elgsena grįstos reklamos tikslais. Žinant šiuos rezultatus, klausimo dėl pasyvaus savisaugos priemonių naudojimo kaip privatumo atsisakymo nebeturėtų kilti. Antra, kalbant apie tokias nesudėtingas savisaugos priemones kaip paslaugų atsisakymą, siekiant išvengti asmens duomenų pateikimo, vėl susiduriama su didelėmis problemomis. Nuomonė, kad asmenys, kurie nepatenkinti verslo subjektų suteikiama duomenų apsauga, gali tiesiog tų paslaugų nenaudoti, yra labai trumparegiška. Šiuo atveju vadovaujamasi nuostata, kad naudojimasis ir nesinaudojimas internete teikiamomis paslaugomis yra lygiaverčiai pasirinkimai. Tačiau dažnai pamirštama, kad naujosios informacinės ir komunikacijų technologijos yra užėmusios svarbų vaidmenį visuomenės gyvenime, todėl

[173] MATZNER, T., *et al*. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 287.

[174] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? Amsterdam Law School Legal Studies Research Paper, 2013, No. 2013-43, p. 43.

[175] Apklausa, atlikta su Nyderlandų karalystės interneto vartotojais, atskleidė, kad 58,6% apklaustųjų mano, jog kompanijoms nėra leidžiama rinkti ir saugoti informaciją apie vartotojų elgesį internete (žr. VAN NOORT, G. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 2014, vol. 32, p. 19). Apklausos, atliktos su Vokietijos interneto vartotojais parodė, kad 33% apklausos dalyvių nežinojo, jog kompanijos kaupia internete apie vartotojus surinktą informaciją ir iš jos sudaro vartotojų profilius (Šaltinis: MATZNER, T., et al. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 287). Tyrimai, atlikti su JAV interneto vartotojais parodo, kad tik 40% apklausoje dalyvavusių asmenų sutiko su teiginiu, kad elektoninio pašto teikėjai skanuoja elektroninių laiškų turinį, kurį panaudoja aktualesnei reklamai. 29% asmenų nurodė, kad taip būti negali, nes elektroninių laiškų skanavimą draudžia įstatymas arba tokia praktika, jeigu būtų, susilauktų didžiulio vartotojų nepasitenkinimo. Pastarieji atsakė neteisingai. (žr. MCDONALD, A. M., CRANOR L. F. *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*. Telecommunications Policy Research Conference, 2010, p. 21 [interaktyvus]. [žiūrėta 2017 m. kovo 17 d.]. Prieiga per internetą: < http://aleecia.com/authors-drafts/tprc-behav-AV.pdf >).

jų naudojimą skatina pačios visuomenės spaudimas. Tai reiškia, kad tam tikrų paslaugų atsisakymas gali reikšti didesnę ar mažesnę žalą asmens socialiniam gyvenimui[176] (pavyzdžiui, su asmeniu, neturinčiu elektroninio pašto bus sunku susisiekti, jam sudėtingiau perduoti informacijos rinkmenas, nesant dalyviu kuriame nors socialiniame tinkle, gali būti sunkiau susirasti darbą ar išlaikyti turimus kontaktus ir pan.). Prieigos prie savo asmens duomenų kitiems sudarymas gali pagausinti asmenų socialinių kontaktų sąrašą, suteikti geresnes karjeros galimybes, todėl vartotojui, ypač neturinčiam jokių žinių apie jo duomenų internete rinkimą ir naudojimą, tai neatrodo joks praradimas. Trečia, asmens duomenų savisaugos priemonės pamažu pačios tampa parduodamais produktais ir paslaugomis. Kaip minėta, yra nemažai priemonių, kurios gali užtikrinti didesnę asmens duomenų apsaugą, tačiau ne visos jos yra nemokamos. Tokie produktai kaip šifravimo programinė įranga įvairiems komunikacijos kanalams, šifruota technika (pvz., mobilieji telefonai, privatūs serveriai), specialūs naršyklės įskiepiai ar abonementinės paslaugos, užtikrinančios duomenų apsaugą, papildomai kainuoja[177]. Vadinasi, dar vienas resursas, reikalingas visapusiškam duomenų savisaugos įgyvendinimui yra papildomos lėšos. Asmenys, kurie, kaip minėta, neturi pakankamai žinių apie duomenų apsaugos poreikį internete, greičiausiai neskubės investuoti į asmens duomenų savisaugos priemones. Viena vertus, ne visi asmenys gali sau leisti papildomas išlaidas duomenų apsaugai. Kita vertus, asmenys nėra linkę mokėti už privatumą dėl įsitikinimo, kad privatumas yra jų teisė, kuri neturėtų būti apmokestinama[178]. Atsižvelgiant į tai, asmens duomenų savisaugos priemonių nenaudojimas neturėtų būti vertinamas kaip sąmoningas savo privatumo atsisakymas. Interneto vartotojai neretai jaučia spaudimą pateikti savo duomenis įvairias paslaugas teikiantiems verslo subjektams, dažnu atveju neturi pakankamų žinių apie duomenų apsaugos poreikį ir priemones ir nemato poreikio joms išlaidauti.

4.2 Asmens duomenų rinkimo ir naudojimo priežiūros problematika

Turint omenyje darbe atlikto tyrimo rezultatus, viešai skelbiamus Valstybinės duomenų apsaugos institucijos prevencinės veiklos rezultatus ir teisinėje literatūroje aprašytus asmens duomenų apsaugą užtikrinančių teisinių reikalavimų nesilaikymo atvejus, svarbu

[176] MATZNER, T., *et al*. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 297.
[177] *Ibid.*, p. 298.
[178] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 44.

paminėti dar vieną dalyką. Atsakomybė už savo asmens duomenų apsaugą negali būti užkraunama vien patiems interneto vartotojams, net jei rinkoje egzistuoja duomenų savisaugos priemonės. Interneto vartotojai ne tik kad neturi pakankamai žinių apie duomenų apsaugą, bet toks rūpestis gali būti didele našta tam tikroms visuomenės grupėms, o kartu, atsižvelgus į šiuo metu egzistuojantį savisaugos priemonių naudojimo mastą, šios priemonės tampa neveiksmingomis.

Jau buvo minėta, kad interneto vartotojų profiliai vartotojų elgsena grįstos reklamos tikslams sudaromi apjungiant duomenis iš įvairių šaltinių, gretinant juos su kitų vartotojų duomenimis ir identifikuojant vartotojų individualius požymius. Tam, kad apie vartotoją ir jo pomėgius būtų padaromos pakankamai patikimos išvados, surinkti duomenys yra veikiami tam tikrų algoritmų ir modulių. O šių technologijų patikimumas ir nuspėjimo tikslumas priklauso nuo duomenų kiekio turimoje duomenų bazėje. Interneto vartotojo elgesio sekimui elektroninėje erdvėje neužtenka tik jo surinktų duomenų, labai svarbu, o gal ir svarbiausia, yra duomenų visuma ir ryšiai, kuriuos iš tos visumos galima nustatyti[179]. Tai reiškia, kad asmens duomenų apsaugos įgyvendinimo problema nėra individuali. Net jeigu vartotojas, turėdamas visą reikalingą informaciją apie pasekmes, sąmoningai nuspręstų pasitikėti verslo subjektais ir leisti vykdyti jo duomenų rinkimą reklamos tikslais (šio asmens teisės šiuo atveju niekaip pažeidžiamos nebūtų), surinkti duomenys vis tiek gali būti panaudojami kitų asmenų (pavyzdžiui, tų, kurie sutikimo nedavė) privatumo pažeidimui[180]. Šiuo aspektu reiktų atkreipti dėmesį, kad būtent dėl to argumentas „neturiu ko slėpti, dėl to mano duomenis gali rinkti kas nori“ yra žalingas ne tik taip teigiančiam asmeniui, bet ir kitiems visuomenės nariams. Kaip tik dėl šios priežasties, esant mažam naudotojų skaičiui, duomenų savisaugos priemonės nėra pakankamai efektyvios asmens duomenų apsaugos užtikrinimui. Jeigu duomenų apsauga būtų išimtinai interneto vartotojų atsakomybė, tai tam, kad apsauga veiktų, į ją turėtų būti žiūrima kaip į socialinę atsakomybę, o ne į asmeninę problemą. Tam būtų reikalinga saviorganizacija ir piliečių valdomi dariniai, kuriantys teisines ir technologines infrastruktūras asmens duomenų savisaugai[181]. Šiuo metu interneto vartotojai nieko panašaus neturi, asmens duomenų savisauga labiau priimama kaip asmeninis rūpestis, todėl interneto vartotojai negali būti laikomi išimtinai atsakingais už savo duomenų apsaugą.

[179] MATZNER, T., *et al*. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 293.
[180] *Ibid.*
[181] *Ibid*., 290.

Kita priežastis, dėl kurios vartotojams negali būti primetama atsakomybė už jų asmens duomenų apsaugą yra susijusi su jau aptartu papildomų resursų poreikiu. Buvo užsiminta, kad resursai (tiek laikas, tiek žinių įsisavinimo galimybė, teik lėšos) visuomenėje yra pasiskirstę nevienodai, todėl beveik neįmanoma savisaugos priemonėmis sukurti vienodai gerų asmens duomenų apsaugos sąlygų visiems interneto vartotojams. Ypatingai kalbant apie papildomų lėšų poreikį, grėsmė šiuo atveju yra ta, kad privatumas gali tapti prabangos preke tiems, kas išgali susimokėti nustatytą kainą[182]. O tiems asmenims, kurie vis dėlto tą kainą sumokėti gali, svarbu priminti, jog ši prabanga iš tiesų neturi jokios realios vertės, jeigu duomenų savisauga neužsiima pakankamai daug asmenų. Be to, labai didelė problema yra ta, kad asmenys, kuriems jų duomenų apsauga yra reikalingiausia (asmenys dažniausiai patiriantys diskriminaciją, pavyzdžiui, LGBT bendruomenės nariai, migrantai, tam tikras religijas išpažįstantys asmenys ir pan.), yra priversti patirti didesnę finansinę ir kitokią naštą, siekdami išvengti su asmens duomenų elektroninėje erdvėje rinkimu ir naudojimu susijusių rizikų[183]. Tokiu būdu vienoms iš jautriausių visuomenės dalių, kurios turi didesnį poreikį asmens duomenų apsaugai elektroninėje erdvėje, uždedama papildoma našta.

Dėl šių priežasčių Europos Sąjungos įgyvendinama duomenų apsaugos reforma su Bendruoju duomenų apsaugos reglamentu priešakyje ir papildomomis iniciatyvomis yra net labai sveikintini žingsniai. Tai reiškia, kad ES yra pasirengusi prisiimti daugiau atsakomybės už interneto vartotojų asmens duomenų rinkimo ir naudojimo pasekmes nei buvo prisiėmusi iki šiol. Vis dėlto, nors iniciatyvos yra sveikintinos, norėtųsi tikėtis, kad duomenų apsaugos reformos teisės aktuose įtvirtintus laimėjimus seks tinkamas jų įgyvendinimas praktikoje tiek ES, tiek nacionaliniu lygmeniu. Kol kas, kol asmens duomenų teisinės apsaugos užtikrinimo internete kontrolės potencialas nėra pilnai išnaudotas, vartotojai neturi kitos išeities kaip savo duomenų rinkimo ir naudojimo kontrole užsiimti patiems. Tačiau net ir šioje vietoje ES ir nacionalinėms institucijoms yra kur pasireikšti – o būtent skatinant interneto vartotojų informuotumą apie vartotojų elgsena grįstos reklamos metodus ir galimas grėsmes jų privatumui. Ypač turint omenyje, kad interneto vartotojų informuotumas yra vienas iš šiuo metu taip trūkstamų resursų asmens duomenų savisaugoje. Žinoma, pasiūlymas institucijoms susirūpinti interneto vartotojų švietimu minėtais klausimais yra gana keblus ir sunkiai priimtinas, kadangi tikėtina, jog išsamiau informuoti vartotojai gali reikšti nepasitenkinimą ne tik duomenis

[182] MATZNER, T., *et al*. Do-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 299.
[183] *Ibid.*

renkančių ir naudojančių verslo subjektų, bet ir pačių institucijų atžvilgiu dėl buvusio ir esamo institucijų neveikimo interneto vartotojų privatumo apsaugos srityje. Todėl, autoriaus nuomone, bent jau iki naujojo BDAR įsigaliojimo, tikėtis, kad interneto vartotojų duomenų rinkimo ir naudojimo veikloje bus matomos kokios nors naujos politinės iniciatyvos (jau nekalbant apie griežtesnę kontrolę ar prevenciją), būtų pernelyg optimistiška. Tačiau tai nereiškia, kad interneto vartotojų informavimo ir švietimo iniciatyvos iš ES ar nacionalinių institucijų yra nelaukiamos po BDAR įsigaliojimo. Paminėta, kad naujajame BDAR įtvirtintose nuostatose kalbama apie vartotojo galimybę priimti būtent informuotą sprendimą dėl jo duomenų rinkimo ir naudojimo. Tam, kad interneto vartotojas galėtų priimti tokį sprendimą, reikalingas ne tik didesnis verslo subjektų skaidrumas duomenis renkant ir naudojant, bet ir žinios apie galimas duoto sutikimo pasekmes, pagaliau net apie galimą vartotojo duomenų vertę[184]. Visiems prieinama ir aiškiai pateikiama ugdomoji informacija suteiktų galią vartotojams sąmoningai nuspręsti dėl savo duomenų likimo, o kartu padėtų plėsti duomenų savisaugą praktikuojančių asmenų gretas.

4.3 Verslo subjektų indėlis į asmens duomenų apsaugą

Ankstesnėje darbo dalyje buvo kalbama apie atsakomybę už asmens duomenų apsaugą ir kontrolę, kuri tenka interneto vartotojams ir turėtų tekti ES ir nacionalinėms duomenų apsaugos priežiūros institucijoms. Šioje dalyje liko aptarti galimą indėlį į interneto vartotojų privatumo užtikrinimą tų subjektų, kurie užsiima duomenų rinkimu ir naudojimu. Be abejo, verslo subjektai, savo veiklą siejantys su vartotojų elgsena grįsta reklama, pirmiausia turėtų tinkamai įgyvendinti teisės aktų jiems priskirtas pareigas asmens duomenų apsaugos srityje (teikti informaciją, prieš renkant duomenis gauti sutikimą, užtikrinti surinktų duomenų saugumą ir pan.). Iš dalies verslo subjektų pasipriešinimas dabar galiojančioms ir būsimoms teisės aktų, reglamentuojančių asmens duomenų rinkimą ir naudojimą, nuostatoms yra logiškas. Interneto vartotojų duomenys yra svarbūs ir vertingi, metų metus užsitęsęs iš esmės nekontroliuojamas jų rinkimas ir netrukdoma vartotojų elgsena grįstos reklamos veikla skatino verslo subjektus investuoti į naujas technologijas, kurios leistų kaupti dar išsamesnę informaciją apie vartotojus. Todėl bet kokios iniciatyvos, ribojančios vartotojų duomenų rinkimą ir naudojimą, buvo ir yra sutinkamos net labai nepalankiai – įvardijant, kad jos kenkia verslui, patiems vartotojams

[184] BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 47.

ir ekonomikai[185]. Pažymėtina kad, nors verslo subjektų nepasitenkinimas yra logiškas, tačiau jis nėra racionalus. Šiuo metu įgyvendinamos duomenų apsaugos reformos tikslas nėra kenkimas verslui ar ekonomikai. Vartotojų elgsena grįsta reklama naujuoju reguliavimu nėra uždraudžiama, yra tik padidinami skaidrumo reikalavimai, taip pat verslui nedaromos jokios kliūtys reklamas interneto vartotojams pateikti kitais metodais. Todėl verslo subjektų pasipriešinimas ar atmestinas požiūris į minėtus teisės aktų reikalavimus turėtų būti traktuojamas kaip paprastas užsispyrimas. Atkreiptinas dėmesys, kad toks elgesys ilgainiui turės neigiamų pasekmių patiems vartotojų elgsena grįsta reklama užsiimantiems subjektams. Be to, kad po BDAR įsigaliojimo jiems grės didelės baudos, svarbus ir vartotojų požiūrio aspektas. Kaip minėta, šiuo metu interneto vartotojų informuotumas apie jų sekimą internete nėra didelis, tačiau jam didėjant gali didėti nepasitenkinimas ir verslo subjektų vykdoma veikla. Toks nepasitenkinimas atneštų daug žalos, nes vartotojai gali nutraukti ryšius su dabartiniais paslaugų tiekėjais ir imti ieškoti alternatyvių šaltinių, kurie negrasina jų privatumui[186]. Arba net imti boikotuoti produktus, kurie reklamuojami naudojant vartotojų elgsena grįstą reklamą. Taigi verslo subjektai šiuo atveju turėtų ne aklai priešintis asmens duomenų teisinio reguliavimo naujovėms, o labiau gerbti interneto vartotojų privatumą. Tikėtina, kad interneto vartotojai, matydami socialiai atsakingesnį elgesį jų privatumo atžvilgiu, priimtiniau reaguos į verslo subjektų vykdomas praktikas ir lengviau duos savo sutikimą duomenų tvarkymui.

Kalbant apie interneto svetainių skelbėjų vaidmenį interneto vartotojų privatumo užtikrinime, paminėtina, kad kai kurie iš jų laikosi praktikos neprileisti vartotojų, įsidiegusių tam tikras savisaugos priemones savo naršyklėje, prie interneto svetainės turinio. Dažniausiai pasitaikantis tokio elgesio pavyzdys – atsidarius interneto svetainę joje atsiranda langas, nurodantis, kad, norint matyti svetainės turinį, reikia išjungti minėtus reklamą ar vartotojų sekimą blokuojančius įskiepius. Kartais interneto vartotojams pateikiama alternatyva – susimokėti nurodytą sumą, kad interneto svetainė būtų matoma be reklamos[187]. Interneto svetainių skelbėjai yra suinteresuoti tokia praktika,

[185] MARKOU, C. Behavioural Advertising and the New 'EU Cookie Law' as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection.* Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 228.

[186] Šiam tikslui labai pasitarnaujanti teisė, įtvirtinta BDAR, yra jau minėta duomenų subjektų teisė į duomenų perkeliamumą (angl. *right to data portability*). Ši teisė reiškia, kad asmenys gali laisvai perkelti savo duomenis iš vieno duomenų valdytojo pas kitą.

[187] Lietuvoje neseniai tokios praktikos ėmėsi naujienų portalas 15min.lt, žr. BALŽEKAS, T. *15min paprašė išjungti reklamos blokavimą. Kokie rezultatai?* 15 min, 2016 m. liepos 20 d. [interaktyvus]. [žiūrėta 2017 m. kovo 19 d.]. Prieiga per internetą: < http://www.15min.lt/naujiena/aktualu/komentarai/tomas-balzekas-15min-paprase-isjungti-reklamos-blokavima-kokie-rezultatai-500-657845 >.

kadangi, kaip jau minėta, daugelis jų didžiąją dalį savo pajamų gauna būtent iš reklamos[188]. Tačiau tokia praktika yra susijusi su tam tikromis problemomis.

Pirmiausia, jeigu dauguma arba visi interneto svetainių skelbėjai reikalautų išjungti reklamą ir vartotojo sekimą internete blokuojančias programas, kitu atveju neprileisdami vartotojų prie turinio, susidarytų situacija, kai vartotojui, kuris suinteresuotas asmens duomenų savisaugos priemonių naudojimu, būtų neprieinama plati dalis internete esančios informacijos. Pavyzdžiui, jeigu visi Lietuvos naujienų tinklalapiai laikytųsi tokios praktikos, interneto vartotojas turėtų pasirinkti, arba būti neinformuotam apie naujienas internete, arba sutikti su primestomis sąlygomis[189]. Jau buvo minėta, kad pasiūlyme dėl Privatumo reglamento yra įtraukta nuostata, jog sutikimas tvarkyti duomenis nebus laikomas galiojančiu, jei duomenų subjektas faktiškai neturi laisvo pasirinkimo arba negali atsisakyti duoti sutikimą ar sutikimo atšaukti, nepatirdamas žalos. Ar ši nuostata išliks ir galutiniame Privatumo reglamento variante, dar nėra aišku. Tačiau jai likus, būtų įdomu pažiūrėti, ar minėtas pavyzdys būtų traktuojamas kaip vartotojo pasirinkimą apribojantis veiksnys.

Antra, tam, kad interneto svetainės skelbėjas žinotų, ar vartotojo galiniame įrenginyje yra konkretus įskiepis, blokuojantis reklamą ar sekimą, ši informacija turi būti patikrinta. Tai yra, interneto svetainės skelbėjas turi pasitelkti tam tikrus metodus, kurie nustatytų vartotojus, savo naršyklėje turinčius jį dominančius įskiepius. Pavyzdžiui, vieno iš populiariausių interneto naršyklės įskiepių *Adblock* aptikimas vartotojo įrenginyje vyksta papildžius interneto svetainės kodo dalį tam tikra užklausa apie vartotojo naršyklę pasiekusią informaciją iš serverio[190]. Kai kurie interneto vartotojų privatumo gynėjai linkę manyti, kad *Adblock* aptikimo vartotojo naršyklėje veiksmai traktuotini kaip skverbimasis į vartotojų galinius įrenginius su tikslu išgauti privačią informaciją apie juos[191]. Todėl imamasi

---

[188] Aiškumo dėlei, paminėtina, kad faktas, jog interneto svetainės skelbėjas blokuoja interneto tinklalapio turinį, nereiškia, kad trečiųjų šalių slapukai ar kitos rinkmenos nėra išsaugomos interneto vartotojo kompiuteryje. Dažniausiai interneto svetainės turinio blokavimas nesustabdo trečiųjų šalių slapukų perkėlimo į vartotojo galinį įrenginį.

[189] Šioje vietoje taip pat galima prisiminti anksčiau skyriuje aptartą galimą interneto vartotojų diskriminaciją pagal pajamas, kai asmenys, turintys papildomų lėšų asmens duomenų apsaugai, gali išvengti savo asmens duomenų tvarkymo, o asmenys tokių lėšų negalintys skirti, turi pasirinkimą tik arba nesinaudoti konkrečia paslauga, arba mainais sutikti su asmens duomenų tvarkymu.

[190] Vartotojui siekiant patekti į tam tikrą interneto svetainę, jis įveda svetainės adresą adreso laukelyje. Tuo metu iš serverio, kur saugomi atitinkamos interneto svetainės duomenys, atsiunčiama įvairi informacija, iš kurios pati svetainė ir susideda (tai HTML tipo failas, kuriame patalpintos išorinės ir vidinės nuorodos į Javascript failus, pakopiniai stilių šablonai (CSS), įvairūs paveikslėliai ir pan.). Kai vartotojas naudoja *Adblock* įskiepį, dalis iš servero siųstos informacijos (kurią sudaro reklama) nepasiekia vartotojo. Jeigu interneto svetainių skelbėjas siekia patikrinti, ar vartotojas naudoja *Adblock* įskiepį, jis minėtame HTML faile padaro papildomą įrašą. Šis įrašas patikrina, ar visa vartotojui iš serverio siųsta informacija pasiekė tą vartotoją. Jeigu aptinkama, kad dalis tam tikros informacijos nebuvo atsiųsta, vadinasi interneto vartotojas turi *Adblock* ar panašų įskiepį (detalesnę informaciją žr. interneto tinklalapyje http://www.detectadblock.com/).

[191] Kaip tai apibūdinta 2002/58/EB direktyvos konstatuojamosios dalies 24 punkte: „<...> *Vadinamieji „šnipukai“, interneto blakės, slaptieji numerio nustatymo įtaisai ir panašūs įtaisai leidžia be naudotojų*

iniciatyvų[192] reikalauti, kad, kaip ir slapukų atveju, taip ir *Adblock* aptikimo metodų naudojimo atveju, iš vartotojų būtų gaunamas aiškus sutikimas (t. y. kad vartotojas sutinka, jog interneto svetainės skelbėjas įsitikintų dėl jo naudojamo įskiepio). Darbo autoriaus vertinimu, toks sutikimo iš vartotojų reikalavimas šiuo atveju yra perteklinis, kadangi aprašyto *Adblock* įskiepio aptikimo metu duomenys iš interneto vartotojo nėra tiesiogiai renkami ir gauta informacija apie vartotojo įskiepį nėra naudojama pažeidžiant jo privatumą[193]. Vis dėlto, ši ir panašios diskusijos tuo klausimu parodo, kad vartotojų naudojamos savisaugos priemonės yra konflikto tarp interneto svetainių skelbėjų ir interneto vartotojų privatumo gynėjų priežastimi.

Kaip jau minėta, asmens duomenų savisaugos priemonės yra naudinga pagalba kovoje prieš asmens privatumo pažeidimus. Daugeliu atveju jos saugo ne tik nuo įkyrių reklamų, bet ir nuo reklama plintančių žalingų rinkmenų[194] bei neteisėto asmens duomenų rinkimo ir naudojimo. Verslo subjektai šiuo atveju neturėtų skatinti interneto vartotojus sumažinti savo apsaugos lygį dėl to, kad būtų prileisti prie svetainės turinio. O tokiu atveju, jeigu kitaip neįmanoma, bent jau turėtų gebėti užtikrinti adekvatų interneto vartotojų įrenginių saugumą ir interneto vartotojų teisę pasirinkti dėl savo duomenų rinkimo ir naudojimo.

Apibendrinant galima pasakyti, kad, nepaisant teigiamų iniciatyvų tobulinti gerokai atgyvenusį teisinį reguliavimą asmens duomenų apsaugos srityje, bendras vaizdas yra slogus (vertinant net ir šiuo metu taikomų, ne tiek daug iššūkių reikalaujančių teisės aktų įgyvendinimą internetinės reklamos srityje). Aiškėja, kad ne tiek ydingas teisinis reguliavimas, kiek šio reguliavimo tinkamo įgyvendinimo stoka, pirmiausia pasireiškianti atsakingų institucijų negebėjimu užtikrinti priežiūrą bei kontrolę, sąlygoja didžiulį asmens

---

žinios įsiskverbti į jų galinius įrenginius siekiant susipažinti su informacija, saugoti slepiamą informaciją ar sekti naudotojo veiksmus, šitaip rimtai pažeidžiant naudotojų privatumą. Tokius įtaisus turėtų būti leidžiama naudoti tik teisėtais tikslais ir kai naudotojas apie tai žino“.

[192] Pavyzdžiui, Alexander Hanff, privatumo aktyvistas ir programuotojas, 2016 metų balandžio mėnesį savo Twitter paskyroje viešai pasidalino Europos Komisijos atsakymu į jo paklausimą, kuriame Europos Komisija patvirtino, jog, jeigu Adblock aptikimo technologijos iš tiesų turi priėjimą prie interneto vartotojų privačių duomenų, jiems turėtų būti taikomas analogiškas vartotojų sutikimo reikalavimo mechanizmas, kaip ir slapukų atveju.

[193] Anksčiau aprašyta *Adblock* aptikimo technologija tiesiogiai duomenų iš interneto vartotojų nerenka, kadangi yra tik tikrinama kaip duomenys iš interneto svetainės skelbėjo serverio pasiekė vartotoją, taigi yra tikrinamas serverio duomenų pasiekiamumas. Pats metodas nėra pagrįstas realios informacijos surinkimu, o tam tikra tikimybe, kad vartotojas vieną ar kitą įskiepį yra įsidiegęs. Tai yra, apie *Adblock* įskiepio turėjimą yra sprendžiama ne iš realių duomenų apie vartotojo naršyklę, o iš požymių (pvz., jeigu tam tikra siųstos informacijos dalis nepasiekė vartotojo, tai labai tikėtina, kad jis turi *Adblock* įskiepį, tačiau iš tiesų apie tai nėra žinoma). Vartotojo įrenginyje išsaugomos informacijos pobūdis ir kiekis sutampa su būtina informacija, kuri išsaugoma kiekvieną kartą aplankius bet kurią interneto svetainę. Taip pat *Adblock* aptikimo veiksmai vykdomi kas kartą iš naujo prisijungus prie tos pačios interneto svetainės, o tai reiškia, kad duomenys apie vartotojų naudojamą įskiepį nėra kaupiami ir saugomi.

[194] Internete pasitaiko atvejų, kai reklamos interneto vartotojams perduoda kenkėjiškas programas (angl. *malware*). Daugiau apie vieną iš tokių atvejų žr. *Malvertising: Daily Mail ads 'briefly linked' to malware*. BBC News, 2015 m. spalio 16 d. [interaktyvus]. [žiūrėta 2017 m. kovo 23 d.]. Prieiga per internetą: <http://www.bbc.com/news/technology-34541915>.

duomenų rinkimo ir naudojimo pažeidimų elektroninėje erdvėje kiekį. Tai neabejotinai verčia baimintis ir dėl naujosios Europos Sąjungos duomenų reformos sėkmės. Tačiau minėta reforma buvo pradėta vykdyti jau turint omenyje svarbiausius asmens duomenų tvarkymo ir apsaugos internete probleminius aspektus, todėl belieka tikėtis, kad nauji teisiniai svertai padės suvaldyti bent jau didžiąją dalį esamų problemų. Modernesnis teisinis reguliavimas bei didesnis dėmesys kartu su socialiai atsakingesniu požiūriu iš interneto vartotojų, verslo subjektų ir priežiūros institucijų turėtų užtikrinti tinkamą balansą tarp teisės į asmens privatumą ir ekonominės gerovės.

IŠVADOS IR PASIŪLYMAI

Išvados

1. Šiuo metu Lietuvoje ir Europos Sąjungoje galiojantis asmens duomenų tvarkymo elektroninėje erdvėje teisinis reguliavimas pasižymi moderniai plačia asmens duomenų samprata ir orientacija į duomenų subjekto sutikimą, kaip pagrindinį asmens duomenų tvarkymo kriterijų, įtvirtinantį duomenų subjekto teisę pasirinkti dėl savo asmens duomenų tvarkymo. Vis dėlto, tiek 95/46/EB direktyvos, tiek ją įgyvendinančio Lietuvos respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimai yra nėra pakankamai pritaikyti elektroninei erdvei ir šiuolaikinėms technologijoms.

2. 2016 metais Europos Parlamento ir Tarybos priimtas Bendrasis duomenų apsaugos reglamentas yra atsakas į technologinį modernėjimą bei daugelio veiklos sričių skaitmenizavimo tendencijas. Bendruoju duomenų apsaugos reglamentu bandomos suvaldyti įvairios rizikos, susijusios su lengviau pažeidžiamu asmenų privatumu, iš esmės pasikeitusiais duomenų tvarkymo principais, itin lengvu asmens duomenų judėjimu tarp valstybių ir tarpusavyje nederančia bei fragmentiška teisine aplinka. Atskiros naujojo reglamento nuostatos gali būti kritikuotinos, bet žvelgiant bendrai, jo priėmimas yra perspektyvus žingsnis asmens duomenų apsaugai Europos Sąjungoje, kuris turėtų ne tik atskleisti bendrosios skaitmeninės rinkos potencialą, bet ir padėti geriau apsaugoti asmenų privatumą.

3. Asmens duomenų rinkimas ir naudojimas elektroninėje erdvėje reklamos tikslais palengva pasidarė neatskiriama naujųjų technologijų ir interneto visuomenės dalis. Tai ypač paveikė interneto vartotojus, kurie vis dažniau tampa internetinio sekimo (angl. *online tracking*) taikiniais. Internetinis sekimas yra vartotojų elgsena grįstos reklamos pagrindas, kuris, pasitelkiant minimalius išteklius ir pastangas, sudaro sąlygas asmenų identifikavimui.

4. Interneto vartotojai paprastai nėra informuojami apie atliekamą jų duomenų rinkimą ir naudojimą, jiems neleidžiama atsisakyti jų asmens duomenų tvarkymo, interneto vartotojai susiduria su apsunkintomis sąlygomis, jeigu pageidauja nutraukti savo atžvilgiu vykdomą internetinį sekimą. Šiuos akivaizdžius teisės aktų pažeidimus sąlygoja ne

ydingas teisinis reguliavimas, o šio reguliavimo tinkamo įgyvendinimo stoka, kuri pasireiškia ir atsakingų institucijų negebėjimu užtikrinti tinkamą priežiūrą ir kontrolę.

5. Asmens duomenų apsaugos elektroninėje erdvėje įgyvendinimo problema nėra individuali. Apie vieną asmenį surinkti duomenys gali būti panaudojami kito asmens privatumo pažeidimui. Todėl, esant mažam naudotojų skaičiui, asmens duomenų savisaugos priemonės nėra pakankamai efektyvios asmens duomenų apsaugos užtikrinimui. Jeigu duomenų apsauga būtų išimtinai interneto vartotojų atsakomybė, tai tam, kad tokia apsauga veiktų, į ją turėtų būti žiūrima kaip į socialiai atsakingą elgesį, o ne kaip į asmeninę problemą.

6. Europos Sąjungos institucijos ir nacionalinės duomenų apsaugos priežiūros institucijos, siekdamos užtikrinti adekvačią asmens duomenų apsaugą ir grąžinti kontrolę interneto vartotojams, privalo tobulinti kontrolės ir priežiūros mechanizmus šioje srityje, taip pat investuoti į interneto vartotojų švietimą privatumo elektroninėje erdvėje klausimais. Tuo tarpu verslo subjektai, rūpindamiesi savo reputacija, į interneto vartotojų asmens duomenų apsaugą turėtų žiūrėti pirmiausia kaip į socialiai atsakingesnį elgesį, t. y. nepiktnaudžiauti naujųjų technologijų teikiamomis galimybėmis, siekiant apeiti teisinį reguliavimą, ir nesikišti į vartotojų vykdomą duomenų savisaugą.

Pasiūlymai

1. Atsižvelgiant į tai, kad šiuo metu Valstybinės duomenų apsaugos inspekcijos prevencinė veikla dėl asmens duomenų rinkimo ir naudojimo elektroninėje erdvėje vykdoma pasyviai bei naudojant neracionalius metodus, siūloma dalį inspekcijos vykdomos prevencinės veiklos perkelti į elektroninę erdvę. Tai reiškia, jog Valstybinės duomenų apsaugos inspekcija turėtų nustatyti teisės aktų pažeidimus ten, kur ir yra vykdoma galimų pažeidėjų veikla – internete. Prevencinė veikla tokiu atveju turėtų vykti naudojantis trečiųjų šalių slapukų ar kitokių interneto vartotojų sekimo priemonių aptikimo programine įranga. Įgyvendinus šį pasiūlymą, atliekami patikrinimai būtų informatyvesni, sumažintų verslo subjektams tenkančią administracinę naštą ir leistų išplėsti tikrinamų subjektų apimtį (o tai taip pat rekomenduotina padaryti).

2. Turint omenyje tai, kad didelė dalis interneto vartotojų apskritai nežino, kad jų duomenys internete yra renkami vartotojų elgsena grįstos reklamos tikslais, siūloma didinti interneto vartotojų informuotumą šioje srityje. Europos Sąjungos ir nacionalinėms duomenų

priežiūros institucijoms siūloma investuoti į interneto vartotojų informuotumą apie vartotojų elgsena grįstos reklamos metodus, iš jų kylančias rizikas privatumui, duodamo sutikimo dėl duomenų tvarkymo svarbą, galimas pasekmes pačiam vartotojui ir kitiems subjektams, taip pat interneto vartotojo duomenų vertę. Įgyvendinus šį pasiūlymą, būtų pasiektas vienas iš asmens duomenų apsaugos teisinio reguliavimo tikslų, kadangi interneto vartotojai galėtų priimti informuotą sprendimą dėl savo duomenų rinkimo ir panaudojimo. Taip pat, informuoti vartotojai galėtų veikti kaip dar vienas kontrolės mechanizmas teisės aktų nuostatų nesilaikantiems duomenų valdytojams ir tvarkytojams.

LITERATŪROS SĄRAŠAS

Teisės norminiai aktai:

1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 1996, Nr. 63-1479;
2. Lietuvos Respublikos elektroninių ryšių įstatymas (su pakeitimais ir papildymais). *Valstybės žinios*, 2004, Nr. 69-2382;
3. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). OL, 2016 L 119, p. 1;
4. Europos Sąjungos pagrindinių teisių chartija. OL, 2012 C 326, p. 391.
5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR. OL, 2016 L 119, p. 89;
6. 2009 m. lapkričio 25 d. Europos Parlamento ir Tarybos Direktyva 2009/136/EB iš dalies keičianti Direktyvą 2002/22/EB dėl universaliųjų paslaugų ir paslaugų gavėjų teisių, susijusių su elektroninių ryšių tinklais ir paslaugomis, Direktyvą 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje ir Reglamentą (EB) Nr. 2006/2004 dėl nacionalinių institucijų, atsakingų už vartotojų apsaugos teisės aktų vykdymą, bendradarbiavimo. OL, 2009 L 337, p. 11;
7. 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo. OL, 1995 L 281, p. 31.

Specialioji literatūra:

8. ALBRECHT, J. P. How the GDPR Will Change the World. *European Data Protection Law Review*, 3/2016, vol. 2, p. 287-289;
9. Asmens duomenų teisinės apsaugos įstatymo komentaras. Vilnius, 2005, p. 14;
10. BLUME, P. Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*, 2012, vol. 2(3), p. 130-136;
11. BOLOGNINI, L., BISTOLF, C. Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to

the new EU General Data Protection Regulation. *Computer Law & Security Review: The International Journal of Technology Law and Practice*, 2016, vol. 33, p. 171-181;

12. BORGESIUS, F. Z. Consent to behavioural targeting in European law - what are the policy implications of insights from behavioural economics? *Amsterdam Law School Legal Studies Research Paper*, 2013, No. 2013-43, p. 1-58;
13. BRKAN, M. Data Protection and Conflict-of-laws: A Challenging Relationship. *European Data Protection Law Review*, 2016, vol. 2, p. 324-341;
14. BURRI, M., SCHÄR, R. The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy. *Journal of Information Policy*, 2016, vol. 6, p. 479-511;
15. CIVILKA, M., ŠLAPIMAITĖ, L. Asmens duomenų samprata elektroninėje erdvėje. *Teisė*, 2015, t. 96, p. 126-148;
16. CRAIG, P., BURCA, G. *EU Law: Text, cases and materials. Sixth Edition*. New York: Oxford University Press, 2015;
17. DAUPARAITĖ, I., *et al*. *Tapatybės vagystė elektroninėje erdvėje: socialiniai, elektroninio verslo ir teisinio reguliavimo aspektai*. Kolektyvinė mokslo monografija. Vilnius: Mykolo Romerio universitetas, 2011;
18. DAVIES, S. The Data Protection Regulation: A Triumph of Pragmatism over Principle? *European Data Protection Law Review*, 3/2016, vol. 2, p. 290-296;
19. HERT, P., PAPAKONSTANTINOU, V. The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer law & security review*, 2016, vol. 32(2), p. 179-194;
20. JENTS, L., KELLI, A. Legal aspects of processing personal data in development and use of digital language resources: the Estonian perspective. *Jurisprudencija*, 2014, 21(1), p. 164-184;
21. KINDT, E. J. Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(5), p. 729-748;
22. LENARD, T. M., RUBIN, P. H. In Defense of Data: Information and the Costs of Privacy. *Technology Policy Institute Working Paper, Emory Law and Economics Research Paper*, 2009, No. 9-44, p. 2-56;
23. MACENAITE, M. From universal towards child-specific protection of the right to privacy online: Dilemmas in the EU General Data Protection Regulation. *New media & society*, 2017, p. 1-15;

24. MARKOU, C. Behavioural Advertising and the New ‘EU Cookie Law’ as a Victim of Business Resistance and a Lack of Official Determination. Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by. S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 213-247;
25. MATZNER, T., *et al. Do*-It-Yourself Data Protection – Empowerment or Burden? Iš *Data Protection on the Move: Current Developments in ICT and Privacy/Data Protection*. Edited by S. Gutwirth, R. Leenes and P. Hert. Law, Governance and Technology, Vol. 24. Belgium: Springer, 2016, p. 277-305;
26. OTT, N., ZYLBERBERG, H. A European Perspective on the Protection of Personal Data in Cyberspace: Explaining How the European Union Is Redefining Ownership and Policies of Personal Data beyond National Borders. *Harvard Kennedy School Review*, 2016, vol. 16, p. 69-75;
27. PETRAITYTĖ, I. Asmens duomenų apsauga ir teisė į privatų gyvenimą. *Teisė*, 2011, t. 80, p. 163-174.
28. REDING, V. The European data protection framework for the twenty-first century. Oxford University Press, *International Data Privacy Law*, 2012, vol. 2, No. 3, p. 119-129;
29. SCHWARTZ, P. M., SOLVE, D. J. The PII problem: privacy and a new concept of personally identifiable information. *New York university law review*, 2011 December, Vol. 86:1814, p. 1814-1894;
30. SKOUMA, G., LÉONARD, L. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Iš *Reforming European Data Protection Law*. S. Gutwirth *et al*. (eds.), Law, Governance and Technology, Vol. 20. Belgium: Springer, 2015, p. 35-60;
31. SWEENEY, L. *Simple Demographics Often Identify People Uniquely*. Data Privacy Working Paper 3. Pittsburgh: Carnegie Mellon University, 2000;
32. TENE, O., POLONETSKY, J. To Track or “Do Not Track”: Advancing Transparency and Individual Control in Online Behavioral Advertising. *Minnesota Journal of Law, Science & Technology*, 2012, vol. 13, No. 1, p. 281-357;
33. VAN NOORT, G. Understanding online behavioural advertising: User knowledge, privacy concerns and online coping behaviour in Europe. *Computers in Human Behavior*, 2014, vol. 32, p. 15-22;
34. VAN WELL, L., ROYAKKERS, L. Ethical Issues in Web Data Mining. *Ethics and Information Technology*, 2004, vol. 6, issue 2, p. 129–140;

35. ZUIDERVEEN BORGESIUS, F. J. Singling out people without knowing their names – Behavioural targeting, pseudonymous data, and the new Data Protection Regulation. *Computer law & security review*, 2016, vol. 32(2), p. 256-271.

Teismų praktika:

36. Europos Sąjungos Teisingumo Teismas. 2016 m. spalio 19 d. sprendimas *Patrick Breyer / Bundesrepublik Deutschland* C‑582/14, ECLI:EU:C:2016:779;
37. Europos Sąjungos Teisingumo Teismas. 2015 m. spalio 1 d. sprendimas *Weltimmo* C-230/14, ECLI:EU:C:2015:639;
38. Europos Sąjungos Teisingumo Teismas. 2014 m. gegužės 13 d. sprendimas *Google Spain and Google* C-131/12, ECLI:EU:C:2014:317;
39. Europos Sąjungos Teisingumo Teismas. 2014 m. balandžio 8 d. sprendimas *Digital Rights Ireland Ltd* C‑293/12 ir *Kärntner Landesregierung* C‑594/12, ECLI:EU:C:2014:238;
40. Europos Sąjungos Teisingumo Teismas. 2014 m. balandžio 8 d. sprendimas *Commission v Hungary* Nr. C-288/12, ECLI:EU:C:2014:237;
41. Europos Sąjungos Teisingumo Teismas. 2011 m. lapkričio 24 d. sprendimas *Scarlet Extended* C‑70/10, ECLI:EU:C:2011:771;
42. Lietuvos Aukščiausiojo Teismo Baudžiamųjų bylų skyriaus teisėjų kolegija. *2015 m. birželio 17 d. nutartis administracinio teisės pažeidimo byloje Valstybinė duomenų apsaugos inspekcija v. R. S. Nr. 2AT-59-976/2015*.

Kita praktinė medžiaga:

43. 29 straipsnio duomenų apsaugos darbo grupės 2007 m. birželio 20 d. priimta „Nuomonė 4/2007 dėl asmens duomenų sąvokos“, 01248/07/LT, WP136, 2007;
44. 29 straipsnio duomenų apsaugos darbo grupės 2010 m. birželio 22 d. priimta „Nuomonė 2/2010 dėl vartotojų elgesiu grindžiamos internetinės reklamos“, 00909/10/LT, WP171, 2010;
45. 29 straipsnio duomenų apsaugos darbo grupės 2010 m. gruodžio 16 d. priimta „Nuomonė 8/2010 dėl taikytinos teisės“, 0836-02/10/LT, WP179, 2010;
46. 29 straipsnio duomenų apsaugos darbo grupės 2011 m. gruodžio 8 d. priimta „Nuomonė 16/2011 dėl EASA / IAB vartotojų elgesiu grindžiamos internetinės reklamos geriausios patirties rekomendacijų“, 02005/11/LT, WP 188, 2011;
47. 29 straipsnio duomenų apsaugos darbo grupės 2011 m. liepos 13 d. priimta „Nuomonė 15/2011 dėl sąvokos „sutikimas“ apibrėžties“, 01197/11/LT WP187, 2011;

48. 29 straipsnio duomenų apsaugos darbo grupės 2012 m. birželio 7 d. priimta „Nuomonė 4/2012 dėl slapukams taikomo reikalavimo gauti sutikimą išimties“, 00879/12/LT, WP 194, 2012;
49. Article 29 Data Protection Working Party. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, 844/14/EN , WP 217, 2014;
50. Article 29 Data Protection Working Party. Opinion 09/2014 on the application of Directive 2002/58/EC to device fingerprinting, 14/EN, WP 224, 2014;
51. European Commision. Commission Staff Working Paper Executive Summary Of The Impact Assessment. Brussels, SEC(2012) 73 final, 2012;
52. European Network and Information Security Agency (ENISA). Privacy considerations of online behavioural tracking, 2012;
53. Europos Komisija. Pasiūlymas dėl Europos Parlamento ir Tarybos Reglamento dėl teisės į privatų gyvenimą ir asmens duomenų apsaugos elektroninių ryšių sektoriuje, kuriuo panaikinama Direktyva 2002/58/EB (Reglamentas dėl privatumo ir elektroninių ryšių). Briuselis, 2017 m. sausio 10 d.;
54. Europos Komisijos komunikatas Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui. Privatumo apsauga glaudžiai susijusiame pasaulyje Europos duomenų apsaugos reglamentavimo pagrindai XXI amžiuje. Briuselis, 2012, COM(2012) 9 final;
55. Valstybinė duomenų apsaugos inspekcija. Internetinių parduotuvių tikrinimų dėl duomenų subjektų teisių įgyvendinimo, asmens duomenų saugojimo teisėtumo ir informacijos saugojimo kliento galiniame įrenginyje ir/ar galimybės naudotis jau saugoma informacija suteikimo teisėtumo rezultatų apibendrinimas, 2012 m. gruodžio 19 d., Nr. 4R-300(17);
56. Valstybinė duomenų apsaugos inspekcija. Paslaugų teikėjų, registruotų valstybinės mokesčių inspekcijos Moss sistemoje, asmens duomenų tvarkymo teisėtumo tikrinimų rezultatų apibendrinimas, 2016 m. gruodžio 29 d.;
57. Valstybinės duomenų apsaugos inspekcija. Rekomendacijos duomenų valdytojams dėl asmens duomenų tvarkymo etikos kodeksų rengimo, 2005.

Elektroniniai dokumentai:

58. ACAR, G., *et al. The Web Never Forgets: Persistent Tracking Mechanisms in the Wild. Study on web tracking mechanisms*. US Princeton University and University of Leuven in

Belgium, 2014 [interaktyvus]. [žiūrėta 2017 m. kovo 14 d.]. Prieiga per internetą: < https://securehomes.esat.kuleuven.be/~gacar/persistent/the_web_never_forgets.pdf >;

59. *Dabartinės lietuvių kalbos žodynas* [interaktyvus]. [žiūrėta 2017 m. vasario 25 d.]. Prieiga per internetą: < http://lkiis.lki.lt/dabartinis >;
60. ECKERSLEY, P. *How Unique Is Your Web Browser?* Electronic Frontier Foundation, 2010 [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < https://panopticlick.eff.org/static/browser-uniqueness.pdf >;
61. ENGLEHARDT, S., NARAYANAN, A. *Online Tracking: A 1-million-site Measurement and Analysis*. Paper of US Princeton University, 2016 [interaktyvus]. [žiūrėta 2017 m. kovo 15 d.]. Prieiga per internetą: http://randomwalker.info/publications/OpenWPM_1_million_site_tracking_measurement.pdf >;
62. *Eurostat newsrelease*, 2016 m. gruodžio 14 d., Nr. 252/2016. [interaktyvus]. [žiūrėta 2017 m. kovo 7 d.]. Prieiga per internetą: < http://ec.europa.eu/eurostat/documents/2995521/7772211/9-14122016-BP-EN.pdf/74f18ee1-07d3-4617-a33c-c84275ac8aa4 >;
63. KRISHNAMURTHY, B., NARYSHKIN, K., WILLS, C. E. *Privacy leakage vs. Protection measures: the growing disconnect*. Web 2.0 Security and Privacy Workshop, 2011 [interaktyvus]. [žiūrėta 2017 m. kovo 1 d.]. Prieiga per internetą: < http://w2spconf.com/2011/papers/privacyVsProtection.pdf >;
64. MCDONALD, A. M., CRANOR L. F. *Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising*. Telecommunications Policy Research Conference, 2010, p. 1-31 [interaktyvus]. [žiūrėta 2017 m. kovo 17 d.]. Prieiga per internetą: < http://aleecia.com/authors-drafts/tprc-behav-AV.pdf >;
65. Statistikos portalas *Statista* [interaktyvus]. [žiūrėta 2017 m. vasario 25 d.]. Prieiga per internetą: < https://www.statista.com/statistics/266206/googles-annual-global-revenue/ > ir < https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/ >;
66. Valstybinės duomenų inspekcijos direktoriaus 2017 m. vasario 06 d. įsakymu Nr. 3R-60 patvirtintas 2017 m. prevencinių tikrinimų planas [interaktyvus]. [žiūrėta 2017 m. kovo 16 d.]. Prieiga per internetą: < https://www.ada.lt/go.php/lit/Prevenciniai-patikrinimai/2 >.

Paminėti žiniasklaidos priemonių šaltiniai:

67. BALŽEKAS, T. *15min paprašė išjungti reklamos blokavimą. Kokie rezultatai?* 15 min, 2016 m. liepos 20 d. [interaktyvus]. [žiūrėta 2017 m. kovo 19 d.]. Prieiga per internetą: < http://www.15min.lt/naujiena/aktualu/komentarai/tomas-balzekas-15min-paprase-isjungti-reklamos-blokavima-kokie-rezultatai-500-657845 >;
68. *Browser 'fingerprints' help track users*. BBC News, 2014 m. liepos 22 d. [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < http://www.bbc.com/news/technology-28423257 >;
69. DUHIGGFEB, C. *How Companies Learn Your Secrets*. New York Times, 2012 vasario 16 d. [interaktyvus]. [žiūrėta 2017 m. kovo 5 d.]. Prieiga per internetą: http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html?_r=2&pagewanted=all?src=tp >;
70. FIORETTI, J. *Facebook wins privacy case against Belgian data protection authority*. Reuters, 2016 birželio 29 d. [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < http://www.reuters.com/article/us-facebook-belgium-idUSKCN0ZF1VV >;
71. FOX-BREWSTER, T. *Google Just Discovered A Massive Web Leak... And You Might Want To Change All Your Passwords*. Forbes, 2017 m. vasario 24 d. [interaktyvus]. [žiūrėta 2017 m. kovo 3 d.]. Prieiga per internetą: https://www.forbes.com/sites/thomasbrewster/2017/02/24/google-just-discovered-a-massive-web-leak-and-you-might-want-to-change-all-your-passwords/#1e6f0c5d3ca3 >;
72. *Yahoo hack: 1bn accounts compromised by biggest data breach in history*. The Guardian, 2016 m. gruodžio 14 d. [interaktyvus]. [žiūrėta 2017 m. kovo 3 d.]. Prieiga per internetą: < https://www.theguardian.com/technology/2016/dec/14/yahoo-hack-security-of-one-billion-accounts-breached >;
73. *Malvertising: Daily Mail ads 'briefly linked' to malware*. BBC News, 2015 m. spalio 16 d. [interaktyvus]. [žiūrėta 2017 m. kovo 23 d.]. Prieiga per internetą: < http://www.bbc.com/news/technology-34541915 >.
74. MATTIOLI, D. *On Orbitz, Mac Users Steered to Pricier Hotels*. The Wall Street Journal, 2012 m. rugpjūčio 23 d. [interaktyvus]. [žiūrėta 2017 m. kovo 8 d.]. Prieiga per internetą: https://www.wsj.com/articles/SB10001424052702304458604577488822667325882 >;
75. *Retargeting Ads Follow Surfers to Other Sites*. New York Times, 2010 m. rugpjūčio 30 d. [interaktyvus]. [žiūrėta 2017 m. vasario 28 d.]. Prieiga per internetą: < http://www.nytimes.com/2010/08/30/technology/30adstalk.html >;
76. WAKEFIELD, J. *What is Facebook doing with my data?* BBC News, 2015 m. spalio 10 d. [interaktyvus]. [žiūrėta 2017 m. kovo 13 d.]. Prieiga per internetą: < http://www.bbc.com/news/magazine-34776191 >.

SANTRAUKA

Naudodamasis internetu asmuo beveik visada palieka savo elgesio pėdsakus. Jeigu tokie duomenys interneto vartotoją identifikuoja ar gali potencialiai identifikuoti, pagal Europos Sąjungos teisinį reguliavimą jie bus laikomi vartotojo asmens duomenimis. Minėtų asmens duomenų rinkimas ir naudojimas elektroninėje erdvėje būtent reklamos tikslais tapo neatskiriama naujųjų technologijų ir interneto visuomenės dalis. Vartotojų elgsena grįsta reklama – tai pagrindinė interneto reklamos rūšis, kuri yra paremta asmens duomenų rinkimu ir naudojimu. Iš vienos pusės, ši reklama padidina verslo subjektams reikalingų vartotojų pasiekiamumą ir padeda parduoti daugiau produktų bei paslaugų. Tačiau, aplinkybė, kad vartotojų elgsena grįstos reklamos veikla dažnai vykdoma nesilaikant skaidrumo, tikslingumo, teisėto tvarkymo pagrindo būtinumo principų, sudaro įspūdį, jog asmenų privatus gyvenimas yra nuolat stebimas.

Darbe siekiama atskleisti svarbiausias interneto vartotojų privatumui kylančias problemas, susijusias su vartotojų elgsena grįsta reklama. Tam, pirmiausia, kryptingai analizuojama asmens duomenų ir jų tvarkymo samprata. Taip pat nagrinėjama asmens duomenų rinkimo ir naudojimo elektroninėje erdvėje teisinė aplinka, t. y. darbo rašymo metu taikomas temai aktualus teisinis reguliavimas ir Europos Sąjungos duomenų apsaugos reformos naujovės. Atliktos teisinės analizės kontekste nagrinėjamos technologinės asmens duomenų rinkimo ir naudojimo galimybės interneto reklamos srityje, o taip pat duomenų subjektų, priežiūros institucijų bei verslo subjektų atsakomybės asmens duomenų apsaugos srityje ribos. Darbe, be kita ko, yra detaliau apžvelgiama viena iš didžiausių teisės asmens duomenų srityje pažeidimus elektroninėje erdvėje sąlygojančių ydų – teisinio reguliavimo tinkamo įgyvendinimo stoka, pasireiškianti ir atsakingų institucijų negebėjimu užtikrinti tinkamą priežiūrą ir kontrolę. Pagaliau, yra pateikiami pasiūlymai esamos situacijos gerinimui.

SUMMARY

Problematic Aspects of Collecting and Processing Personal Data in Cyberspace

A person almost always leaves some traces while using internet. According to European Union law, in case such data identifies or can potentially identify a person, it is assigned to a legal category of personal information. The collection and usage of mentioned personal data in online advertising has become an integral part of an internet-driven society. Behavioural advertising is the main type of online advertising which is based on collecting and processing of personal data. On the one hand, this type of advertising allows marketers to reach a more receptive audience and sell more products or services. However, behavioural advertising is often performed without principles of transparency, fairness for specified purposes and legitimate basis laid down by law. That generates in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.

The aim of this Master thesis is to reveal the most important problematic aspects in terms of internet privacy related to behavioural advertising. For this reason, firstly the conception of personal data and data processing in cyberspace is analysed. Then, the focus is put on currently applicable law relating processing and collecting of personal data as well as new rules of EU Data Protection Reform. The performed analysis is used to examine technical means of personal data collection and usage in online advertising, also to identify the scope of responsibility of data protection that should be assigned to data subjects, supervisory authorities and business representatives. Furthermore, the Master thesis, among other things, reveals one of the biggest defects in personal data protection related to online advertising – the deficiency of appropriate implementation which is also caused by inability of responsible institutions to ensure effective supervision and control. Finally, suggestions for improvement of the situation are presented.

PRIEDAS

Praktinis tyrimas

Tikslas. Tyrimas atliktas siekiant nustatyti, kaip trys lankomiausi lietuviški naujienų tinklalapiai laikosi 95/46/EB direktyvos ir vadinamojo „ES slapukų įstatymo“ nuostatų.

Priemonės ir tyrimo objektas. Darbo autorius atlieka tyrimą, naudodamasis *Google Chrome* naršykle. Naršyklės privatumo nustatymuose darbo autorius pasirinko blokuoti visus trečiųjų šalių siunčiamus slapukus ir kitus tinklapių siunčiamus duomenis (angl. *block third-party cookies and site data*). Naršyklėje yra įdiegtas įskiepis *Privacy Badger*[195], kuris seka ir blokuoja vartotojui iš interneto svetainių siunčiamus trečiųjų šalių slapukus ir kitas sekimo rinkmenas. Tyrimui pasirinkti trys lankomiausi[196] lietuviški naujienų tinklalapiai – delfi.lt, 15min.lt ir lrytas.lt. Tyrimas atliekamas su kiekvienu iš tinklalapių atskirai.

Planuojama tyrimo eiga. Į interneto naršyklės adreso lauką įvedamas tinklalapio adresas. Laukiama, kol susigeneruos tinklalapio turinys ir pasirodys pranešimas apie interneto svetainėje naudojamus slapukus. Darbo autoriaus tikslas, apsilankius kiekviename iš tinklalapių, išvengti trečiųjų šalių slapukų įrašymo į darbo autoriaus naršyklę, t. y. nė vienam iš aplankytų interneto tinklalapių neduoti sutikimo naudoti trečiųjų šalių slapukus.

	Delfi.lt	**15min.lt**	**lrytas.lt**
Prisijungimo metu bandyta išsaugoti[197] trečiųjų šalių slapukų ir kitų rinkmenų iš viso:	18	12	18
Pasirodė informacinis pranešimas apie tinklalapyje naudojamus slapukus:	Ne[198]	Taip[199]	Taip[200]
Prieš vartotojo kompiuteryje bandant išsaugoti trečiųjų šalių slapukus buvo paprašyta vartotojo sutikimo:	Ne	Ne	Ne

[195] *Privacy Badger* – tai naršyklės įskiepis, kuris sustabdo trečiųjų šalių atliekamą interneto vartotojo sekimą, prieš tai parodydamas tų trečiųjų šalių informaciją. Daugiau informacijos apie įskiepį žr. interneto tinklalapyje https://www.eff.org/privacybadger.

[196] Pagal UAB Gemius Baltic atliktus skaičiavimus, žr. interneto tinklalapį http://www.gemius.lt/visos-naujienos/i-lankomiausiu-portalu-trejetuka-sugrizo-lrytaslt.html.

[197] Trečiųjų šalių slapukai ir kitos rinkmenos darbo autoriaus kompiuteryje neišsaugotos tik dėl *Privacy Badger* blokavimo, o ne kitų išorinių veiksnių.

[198] Šiuo atveju pranešimas apie tinklalapio politiką nepasirodė dėl to, kad įskiepio *Privacy Badger* trečiųjų šalių slapukų blokavimas iškraipo visą puslapio vaizdą ir neleidžia jam pilnai užsikrauti.

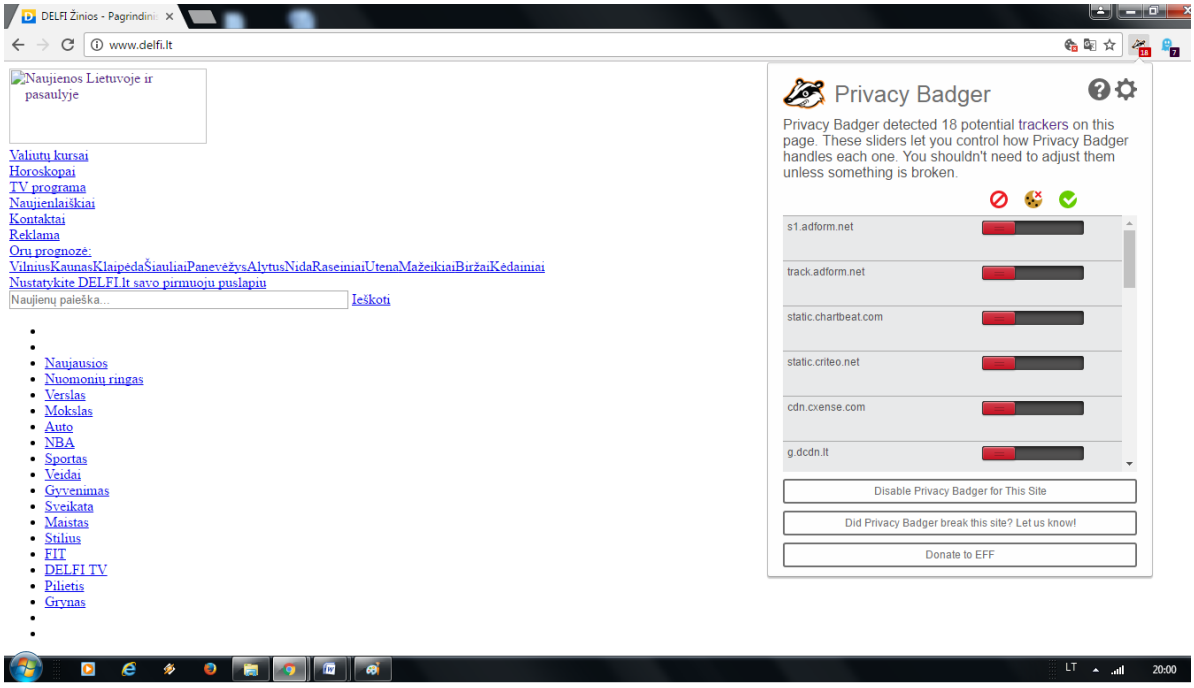
[199] Pranešime nurodyta: „Svetainėje naudojami slapukai, kurie padeda užtikrinti jums teikiamų paslaugų kokybę. Tęsdami naršymą jūs sutinkate su *15min* slapukų politika“.

[200] Pranešime nurodyta: „Norėdami pagerinti Jūsų naršymo kokybę, naudojame slapukus, kuriuos galite bet kada atšaukti“.

Prieš vartotojo kompiuteryje bandant išsaugoti slapukus vartotojas buvo informuotas apie trečiąsias šalis, siunčiančias slapukus, ir jų tikslus:	Ne	Ne	Ne

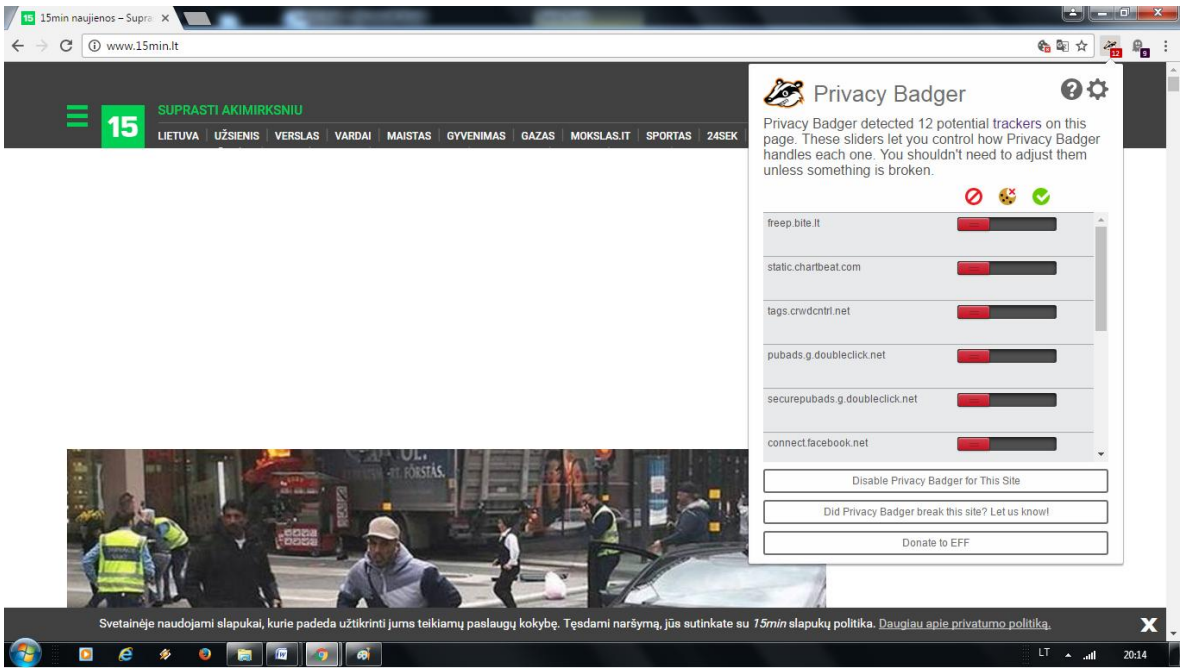
Rezultatai. Visi trys aplankyti tinklalapiai darbo autoriaus kompiuteryje bandė išsaugoti trečiųjų šalių slapukus ar kitas rinkmenas prieš tai neklausę dėl autoriaus sutikimo, neinformavę apie trečiąsias šalis, kurios bando išsaugoti slapukus. Taip pat dvejuose iš trijų tinklalapių pasirodė interneto vartotojus klaidinantys internetiniai pranešimai, kuriuose teigiama, kad slapukai tinklalapiuose naudojami vien dėl naršymo ar paslaugų teikimo kokybės užtikrinimo[201]. Papildomai pažymėtina, kad naršyklės privatumo nustatymai šiuo atveju trečiųjų šalių slapukų ir kitų rinkmenų išvengti nepadėjo.

Vaizdinė medžiaga.



1 paveikslas. Prisijungimo prie delfi.lt metu interneto vartotojo įrenginyje buvo bandoma išsaugoti 18 trečiųjų šalių slapukų ir kitų rinkmenų.

[201] Galima spręsti, kad tinklalapiuose pasirodę pranešimai daro nuorodas į pirmosios šalies slapukus (t. y. interneto vartotojas gali suprasti, kad tinklalapyje yra naudojami tik pirmosios šalies slapukai), tačiau pažymėtina, kad šiame tyrime buvo skaičiuojami tik nuolatinio pobūdžio trečiųjų šalių slapukai.



2 paveikslas. Prisijungimo prie 15min.lt metu interneto vartotojo įrenginyje buvo bandoma išsaugoti 12 trečiųjų šalių slapukų ir kitų rinkmenų.

3 paveikslas. Prisijungimo prie lrytas.lt metu interneto vartotojo įrenginyje buvo bandoma išsaugoti 16 trečiųjų šalių slapukų ir kitų rinkmenų.