MYKOLO ROMERIO UNVERSITETAS

MYKOLO ROMERIO TEISĖS MOKYKLA

PRIVATINĖS TEISĖS INSTITUTAS

JULIJA ZORINA

CIVILINĖS IR VERSLO TEISĖS STUDIJŲ PROGRAMA

ASMENS DUOMENŲ ANONIMIZAVIMAS

(PERSONAL DATA ANONYMIZATION)

Magistro baigiamasis darbas

Darbo vadovas –

Prof. dr. Paulius Pakutinskas

Vilnius, 2019

TURINYS

ĮVADAS

Teisė į asmens duomenų apsaugą – tai viena pagrindinių asmens teisių įtvirtintų Europos Sąjungos pagrindinių teisių chartijoje, kuri nurodo, kad „kiekvienas turi teisę į savo duomenų apsaugą“[1]. Taip pat teisę į privatų gyvenimą užtikrina ir kiti teisės aktai, tokie kaip Visuotinė žmogaus teisių deklaracija (12 straipsnis)[2], Europos žmogaus teisių konvencija (8 straipsnis)[3], Lietuvos Respublikos Konstitucija (22 straipsnis)[4], Lietuvos Respublikos civilinio kodekso (toliau – LR CK) 2.23 straipsnis[5] ir kt. Tikriausiai didžiausio visuomenės susidomėjimo asmens duomenų apsauga sulaukė 2018 m. gegužės 25 d. įsigaliojus Bendrajam duomenų apsaugos reglamentui (toliau – BDAR arba Reglamentas), kuris sustiprino iki tol buvusį asmens duomenų apsaugos reguliavimą, sugriežtino duomenų tvarkymo taisykles ir ženkliai padidino piniginės baudas už Reglamento taisyklių nesilaikymą[6]. Natūralu, kad sugriežtinus asmens duomenų apsaugos reikalavimus išaugo ir duomenų valdytojo atsakomybė už tuos asmens duomenis, kuriuos jis tvarko. Atsižvelgiant į tai, duomenų valdytojui yra reikalingi teisiniai-techniniai sprendimai, kurių pagalba jis galės tvarkyti asmens duomenis nepažeidžiant teisės aktų reikalavimų ir nesukeliant duomenų apsaugos pažeidimo rizikos. Vienas tokių sprendimų yra asmens duomenų anonimizavimas, kuris plačiai bus analizuojamas šiame darbe.

***Tiriamoji problema*.** Šiame darbe tiriama viena iš asmens duomenų saugumo priemonių – asmens duomenų anonimizavimas. Gilinamasi į asmens duomenų anonimizavimo pagrindinius aspektus, sampratą bei paskirtį. Tiriami asmens duomenų anonimizavimo metodai, vertinami jų privalumai bei trūkumai, taip pat lyginami ir atribojami nuo kitų duomenų saugumo priemonių. Analizuojant šiuos ir kitus aspektus, siekiama atsakyti į klausimą: kaip asmens duomenų anonimizavimu užtikrinama duomenų apsauga ir kuo jis skiriasi nuo kitų duomenų saugumo priemonių?

***Baigiamojo darbo aktualumas*.** Įsigaliojus Bendrajam duomenų apsaugos reglamentui buvo sugriežtinti asmens duomenų tvarkymo reikalavimai. Natūralu, kad sugriežtinus minėtus reikalavimus išaugo ir duomenų valdytojo atsakomybė už tvarkomus asmens duomenis. Atsižvelgiant į tai, duomenų valdytojas suinteresuotas tvarkyti asmens duomenis tokiu būdu, kad jam nekiltų

[1] „Europos Sąjungos pagrindinių teisių chartija (2016/C 202/02)“, *Europos Sąjungos oficialus leidinys*, (2016).
[2] „Visuotinė žmogaus teisių deklaracija“, *Valstybės žinios*, (2006).
[3] „Europos žmogaus teisių konvencija“, *Valstybės žinios*, (1995).
[4] „Lietuvos Respublikos Konstitucija“, *Lietuvos Aidas*, (1992).
[5] „Lietuvos Respublikos civilinis kodeksas“, *Valstybės žinios*, (2000).
[6] „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)“. *Europos Sąjungos oficialusis leidinys*, (2016).

duomenų pažeidimo rizika ir tuo pačiu išsaugant savo galimybes pasiekti atitinkamų tvarkymo tikslų. Siekiant vieno ar kito tikslo, tam tikrais atvejais nėra būtina tvarkyti asmenį identifikuojančius duomenis. Pavyzdžiui tuo atveju, kai asmens duomenis tvarkomi statistiniais arba mokslinių, istorinių tyrimų tikslais, yra svarbus tik atitinkamas iš tokių duomenų pasiektas rezultatas, išvada ir tokį tikslą įgyvendinus asmens identifikavimas tampa perteklinis. Tokiu atveju duomenų valdytojas turi laikytis duomenų apsaugos reikalavimų ir perteklinius duomenis sunaikinti arba anonimizuoti. Kadangi sunaikinus asmens duomenis, duomenų valdytojas praranda ir savo galimybes tvarkyti duomenis atitinkamais tikslais, naudingiau jam būtų asmens duomenis anonimizuoti. Asmens duomenų anonimizavimas galėtų leisti pasiekti pusiausvyrą tarp asmens duomenų apsaugos reikalavimų ir duomenų valdytojo lūkesčio išlaikyti atitinkamą informaciją apie duomenų subjektus. Tačiau šiai dienai asmens duomenų anonimizavimas nėra taip plačiai žinomas bei taikomas praktikoje kaip pavyzdžiui pseudominizavimas ir šifravimas, kurie yra tiesiogiai įtvirtinti Reglamente. Atsižvelgiant į tai, šiai dienai yra itin aktualu atskleisti kaip asmens duomenų anonimizavimas gali užtikrinti duomenų apsaugą, taip pat kaip gali padėti išlaikyti duomenų valdytojo galimybes tvarkyti atitinkamus duomenis.

Baigiamojo darbo mokslinis naujumas. Kalbant apie asmens duomenų apsaugą, ši teisės sritis kol kas dar nėra labai plačiai išnagrinėta bei pakankamai žinoma visuomenėje, ypač turint omenyje, jog nauji asmens duomenų apsaugos reikalavimai įsigaliojo šiek tiek daugiau nei prieš metus ir asmens duomenų apsauga kai kuriems duomenų valdytojams vis dar yra naujovė. Kalbant apie asmens duomenų anonimizavimą, šis procesas yra dar mažiau žinomas bei taikomas praktikoje. Siekiant apdoroti asmens duomenis tokiu būdu, kad išnyktų galimybė nustatyti atitinkamo asmens tapatybę ir tuo pačiu išsaugant galimybes pasiekti atitinkamų tikslų, galima pasinaudoti asmens duomenų anonimizavimo metodais. Tačiau šiai dienai nei minėti metodai, nei asmens duomenų anonimizavimo apibrėžimas nėra tiesiogiai įtvirtinti nei Reglamente, nei kitame duomenų apsaugą reglamentuojančiame teisės akte Lietuvos lygmeniu. Be to, doktrinoje taip pat nėra pateikiama bendrai susisteminta informacija apie asmens duomenų anonimizavimą, kuri apimtų jo sampratą, paskirtį, taikomų metodų turinį bei skirtumus nuo kitų duomenų saugumo priemonių.

Baigiamajame darbe tiriamos problemos ištyrimo lygis. Bendrasis duomenų apsaugos reglamentas numato kelias duomenų saugumo priemones, tačiau asmens duomenų anonimizavimas nėra minimas tarp jų. Apskritai nei Reglamentas, nei kitas LR įstatymas nepateikia asmens duomenų anonimizavimo apibrėžimo. Pagrindinius asmens duomenų nuasmeninimo (anonimizavimo) metodus buvo atskleidusi Valstybinė duomenų apsaugos institucija savo 2015 m. rekomendacijoje

dėl nuasmeninimo metodų[7], taip pat Europos Komisijos 29 straipsnio duomenų apsaugos darbo grupės parengtoje Nuomonėje 05/2014 dėl nuasmeninimo metodų[8]. Taip pat asmens duomenų anonimizavimo metodai, vertinant juos iš techninės pusės, buvo dalinai atskleisti Vytauto didžiojo universiteto studentės Jūratės Baltrūkėnaitės magistriniame darbe *„Kokybinių socialinių apklausų anonimizavimo modelis“*[9] ir užsienio literatūroje tokių autorių kaip Josep Domingo-Ferrer, David Sánchez, Jordi Soria-Comas[10]. Asmens duomenų anonimizavimo sąvoka buvo nustatoma tokių autorių kaip Balaji Raghunathan[11], Catherine Tessier, Vincent Bonnemains[12] ir kt.. Tačiau vieno susisteminto šaltinio, kur būtų atskleista asmens duomenų anonimizavimo ir jo elementų sampratos, taip pat jo taikomų metodų turinys bei skirtumai nuo kitų duomenų saugumo priemonių, nėra. Taip pat nebuvo tirti asmens duomenų anonimizavimo bei teismo procesinių sprendimų ar kitų dokumentų nuasmeninimo panašumai ir skirtumai.

Baigiamojo darbo reikšmė. Susisteminta informacija apie asmens duomenų anonimizavimą, jos atribojimą nuo kitų duomenų saugumo priemonių bei anonimizavimo metodų patikimumo vertinimą gali būti naudinga priemonė mokslo tyrėjams, kurie nagrinėja asmens duomenų anonimizavimo procesą, taip pat ir kitiems asmenims, siekiantiems gauti išsamią informaciją apie asmens duomenų anonimizavimą. Ištirus bei susisteminus reikšmingą informaciją apie asmens duomenų anonimizavimą, ji taip pat gali būti naudinga duomenų valdytojams renkantis duomenų saugumo priemonę, kuri galės užtikrinti duomenų subjekto anonimiškumą. Atribojant asmens duomenų anonimizavimą nuo kitų duomenų saugumo priemonių, tokių kaip pseudomonizavimas, šifravimas ir teismo procesinių sprendimų nuasmeninimas tai gali padėti išvengti klaidingų tapatinimų su kitomis duomenų saugumo priemonėmis ir turėti įtakos renkantis tinkamą duomenų saugumo priemonę. Be to, atskleidus bei įvertinus asmens duomenų anonimizavimo metodų turinius, tai gali palegvinti duomenų valdytojui apsispęsti, kurį iš asmens duomenų anonimizavimo metodų jam būtų tinkamiausia taikyti jo konkrečiu atveju. Taip pat šis darbas gali būti reikšmingas teisės aktų leidėjams tobulinant dabartinį Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą[13], taip pat ir kitus asmens duomenų apsaugą reglamentuojančius

---

[7] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“*, 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf

[8] Europos Komisija, *Nuomonė 05/2014 dėl nuasmeninimo metodų*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf

[9] Jūratė Baltrukėnaitė, *„Kokybinių socialinių apklausų anonimizavimo modelis“*, (magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2019). Prieiga per internetą: https://www.vdu.lt/cris/bitstream/20.500.12259/79175/1/Jurate_Baltrukenaite_md.pdf

[10] Josep Domingo-Ferrer, David Sánchez, Jordi Soria-Comas, „*Database Anonymization – Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections“*. (Morgan & Claypool Publishers, 2016)

[11] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf

[12] Catherine Tessier, Vincent Bonnemains, *„Neuroergonomics“*, (Academic Press, 2018)

[13] „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, *TAR*, (2018)

teisės aktus, siekiant apibrėžti dar vieną duomenų saugumo priemonę – asmens duomenų anonimizavimą.

Tyrimo tikslas. Ištirti asmens duomenų anonimizavimo sampratą bei galimybę užtikrinti duomenų apsauga pasitelkiant anonimizavimu.

Tyrimo uždaviniai:

1. Ištirti asmens duomenų anonimizavimo sampratą, taip pat atskleisti jos paskirtį ir pagrindinius reikalavimus.

2. Atriboti asmens duomenų anonimizavimą nuo kitų duomenų saugumo priemonių, tokių kaip pseudominizavimas, šifravimas ir teismo bylų nuasmeninimas.

3. Ištirti pagrindinius asmens duomenų anonimizavimo metodus, nustatyti kiekvieno jų turinį ir įvertinti jų privalumus bei trūkumus.

Tyrimo metodika. Rengiant mokslinį darbą buvo naudojami šie tyrimo metodai:

1. Sisteminės analizės metodas. Sistemiškai vertinant skirtingų autorių teiginius ir teisės aktuose pateiktus apibrėžimus buvo nustatomos asmens duomenų, anoniminių duomenų ir anonimizavimo sampratos. Šis metodas taip pat buvo taikomas siekiant atriboti anoniminius duomenis nuo asmens duomenų ir nustatyti jų teisinį ryšį, taip pat atribojant anonimizavimą nuo pseudominizavimo, šifravimo ir teismo bylų nuasmeninimo.

2. Teisės aktų, teismų praktikos, mokslo doktrinos, mokslinių straipsnių analizė. Teisės aktų analizė buvo taikoma nustatant asmens duomenų apsaugai taikomą teisinį reglamentavimą, taip pat atsakant į klausimą kokia teisinė apsauga yra taikoma anoniminiams duomenims. Lietuvos ir Europos Sąjungos teismų praktika buvo naudota pateikiant asmens duomenų pavyzdžius, taip pat pateikiant netinkamo anonimizavimo pavyzdžius, teismo bylų nuasmeninimo pavyzdžius. Nustatant asmens duomenų anonimizavimo paskirtį, pagrindinius reikalavimus bei taikomus anonimizavimo metodus buvo analizuojama Lietuvos ir užsienio mokslo doktrina, taip pat moksliniai straipsniai.

3. Lyginamosios analizės metodas buvo naudotas lyginant skirtingų autorių mintis dėl asmens duomenų sampratos elementų, siekiant nustatyti požymius pagal kuriuos būtų galima aiškiai atriboti asmens duomenis nuo kitokios informacijos. Taip pat šis metodas buvo naudojamas lyginant anonimizavimo metodus, nustatant jų trūkumus ir privalumus, taip pat vertinant kokioje situacijoje būtų geriausiai taikyti atitinkamą metodą. Atribojant anonimizavimą nuo kitų duomenų saugumo priemonių taip pat buvo naudojamas lyginamasis metodas.

4. Sintezės metodo pagalba buvo jungiami mokslininkų pasisakymai dėl asmens duomenų anonimizavimo sąvokos, siekiant nustatyti išsamų asmens duomenų anonimizavimo apibrėžimą. Taip pat šiuo metodu buvo nustatomi anoniminių duomenų požymiai.

5. Genetinis metodas buvo naudotas siekiant ištirti asmens duomenų apsaugos atsiradimą ir tolesnį vystymą.

6. Analogijos metodas buvo taikomas siekiant nustatyti kuriuo požiūrio laikomasi Lietuvoje kalbant apie vieną iš asmens duomenų anonimizavimui taikomą reikalavimą – negalėjimą nustatyti asmens tapatybes.

7. Apibendrinimo metodas buvo taikytas apibendrinant skirtingų autorių mintis, taip pat siekiant pateikti kiekvienos išanalizuotos dalies išvadą.

Tyrimo struktūra. Mokslinį darbą sudaro: įvadas, trys dėstomosios dalys, išvados, pasiūlymai. Pirmoje dėstomojoje dalyje nustatomi pagrindiniai asmens duomenų anonimizavimo aspektai, tokie kaip anonimizavimo samprata, jo paskirtis ir pagrindiniai taikomi reikalavimai, taip pat asmens duomenų ir anoniminių duomenų sampratos. Taip pat šioje dalyje nagrinėjamas asmens duomenų ir anoniminių duomenų teisinis ryšys, šių sampratų teisinio reglamentavimo skirtumai ir jų vaidmuo asmens duomenų anonimizavimo procese. Antroje mokslinio darbo dalyje siekiama nustatyti kitų duomenų saugumo priemonių sampratą, plačiai išnagrinėti tokias priemones kaip pseudominizavimas, šifravimas ir teismo bylų nuasmeninimas, siekiant atriboti minėtas duomenų saugumo priemones nuo asmens duomenų anonimizavimo. Trečioje šio darbo dalyje nagrinėjami asmens duomenų anonimizavimo metodai, ištiriamas ir plačiai atskleidžiamas kiekvienas metodas, jo taikymo galimybės, taip pat vertinami kiekvieno metodo privalumai bei trūkumai.

Ginamieji teiginiai.

1. Asmens duomenų anonimizavimas yra duomenų saugumo priemonė, kuri gali užtikrinti duomenų subjektui visišką ir negrįžtamą anonimiškumą.
2. Asmens duomenų anonimizavimo negalima tapatinti su kitomis duomenų saugumo priemonėmis, tokiomis kaip pseudominizavimas, šifravimas bei nuasmeninimas.

1. ASMENS DUOMENŲ ANONIMIZAVIMO PAGRINDINIAI ASPEKTAI

1.1. Asmens duomenų samprata

„1890 m. JAV teisininkai S.Warrenas ir L.Brandeisas parašė darbą apie asmens teisę į privatumą ir apibrėžė ją kaip „teisę būti paliktam vienam“. Jie pirmieji išreiškė privatumą kaip didžiulę socialinę vertybę, kuri turi būti saugoma įstatymo ir teisėjų. Vėliau privatumo koncepcija plėtojosi kita linkme ir šiuo metu privatumas dažnai tapatinamas su duomenų apsauga“[14]. „Vienas iš akademinių duomenų apsaugos teisės krikštatėvių F.V. Hondijus duomenų apsaugą apibrėžė kaip asmenų teisių, laisvių ir svarbiausių interesų apsaugą tvarkant su asmenims susijusią informaciją, ypač tai darant naudojami kompiuteriai. Šiuolaikinė teisės doktrina duomenų apsaugą apibrėžia kaip priemonių (ir teisinių, ir neteisinių), kuriomis siekiama apsaugoti asmenis nuo žalos, kurią nulemia informacijos apie tuos asmenis tvarkymas (ir kompiuterizuotas, ir rankinis), ir kurios apima tam tikrus asmeninės informacijos tvarkymo principus, sistemą“[15].

Prieš kalbant apie asmens duomenų anonimizavimą kaip apie procesą, pirmiausia reikėtų tiksliai nustatyti jo sudedamąsias dalis. Viena iš tokių dalių yra asmens duomenys. Kadangi šio darbo tyrimo objektas yra būtent asmens duomenų anonimizavimas, toliau šiame skyriuje bus nustatoma asmens duomenų samprata ir jos elementai. Atkreiptinas dėmesys, kad asmens duomenų sampratos elementai, tiksliau jų (ne)buvimas, bus svarbūs nustatant ar atitinkamas duomenų rinkinys bus laikomas tinkamai anonimizuotu ar ne. Kitaip tariant asmens duomenys turi svarbų vaidmenį asmens duomenų anonimizavimo procese, todėl jų sampratą būtina atskleisti.

Bendrasis duomenų apsaugos reglamentas pateikia asmens duomenų apibrėžimą: „asmens duomenys – tai bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti“[16]. Analizuojant šį Reglamento straipsnį būtų galima išskirti du pagrindinius asmens duomenų sąvokos elementus. Visų pirma, informacija turi būti apie fizinį asmenį ir antra – reikalingas tapatybės nustatymas, tiesioginis arba netiesioginis. Pasak Mindaugą Civilką tapatybės nustatymas gali būti dvejopas, t.y. 1) tiesioginis – asmens vardas, pavardė, asmens kodas ir tt. ir 2) netiesioginis – asmeniui būdingi fiziniai, fiziologiniai, protiniai, kultūriniai, ekonominiai,

---

[14] Darius Štitilis, Mindaugas Kiškis, Tadas Limba, *„Interneto ir technologijų teisė“*. (Vilnius: Registrų centras, 2016), 328 psl.

[15] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 29 psl. Cituota iš Hondius, W. Frits, „*Data Law in Europe. Stanford Journal of International Law“*, (1980), Vol. 16, p. 89.

[16] „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)“. *Europos Sąjungos oficialusis leidinys*, (2016).

socialiniai tapatybės veiksniai[17]. Interneto ir technologijų teisės vadovėlyje rašoma, jog „duomenys gali būti asmeniniai netgi tada, jeigu juos pasitelkus asmuo gali būti identifikuotas tik turint kitų duomenų kombinaciją – pagalbinius duomenis“[18]. Tačiau tai, ar atitinkama informacija tiesiogiai arba netiesiogiai nustato asmens tapatybę, ar ne, turi būti nustatoma kiekvienu konkrečiu atveju atsižvelgiant į konkrečias aplinkybes[19]. Europos Komisija (toliau – EK) taip pat pateikia asmens duomenų apibrėžimą: „asmens duomenys yra bet kokia informacija, susijusi su gyvu asmeniu, kurio tapatybė yra nustatyta arba gali būti nustatyta. Skirtinga informacija, kuri surinkta kartu gali atskleisti konkretaus asmens tapatybę, taip pat yra asmens duomenys“[20]. Šis apibrėžimas iš esmės yra identiškas Reglamente nustatytam, tačiau šiuo atveju be jau ankstesnių išskirtų požymių, galima išskirti dar vieną – fizinis asmuo turi būti gyvas, t.y. asmens duomenų sąvoka neapima mirusiųjų asmenų duomenų. Taip pat dar kartą pabrėžiama, jog tokia informacija gali būti surinkta nebūtinai iš vieno šaltinio.

Siekiant aiškiai atskirti asmens duomenis nuo bet kokių kitų duomenų arba informacijos, svarbu nustatyti aiškius asmens duomenų sampratos elementus. Julius Zaleskis monografijoje „Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“ remdamasis Europos Komisijos Nuomone 4/2007 dėl asmens duomenų sąvokos išskyrė keturis asmens duomenų sampratos elementus[21]. Jis rašė: „galima skirti keturis duomenų sampratos elementus, kurie yra glaudžiai susiję ir priklausomi vienas nuo kito. Duomenų apsaugos teisės normos taikomos, jeigu nustatoma, kad yra visi elementai“[22]. Šie keturi elementai yra: 1) informacijos samprata; 2) informacijos sąsajumas su asmeniu; 3) fizinio asmens samprata; 4) galimybė nustatyti tapatybę[23]. Toliau bus plačiau aptariamas kiekvienas iš šių elementų.

Pirmas elementas – informacijos samprata. Kaip nurodyta J. Zaleskio monografijoje „duomenys – tai bet kokia informacija. [...] Tai ir objektyvi informacija, pavyzdžiui tam tikros medžiagos buvimas asmens kraujyje, ir subjektyvi informacija – nuomonės arba vertinimai. Kad informacija būtų laikoma duomenimis, ji neturi būti teisinga ar įrodyta. Iš ES Teisingumo Teismo jurisprudencijos matyti, kad aplinkybė, jog konkreti informacija priskirtina profesinės veiklos sričiai,

---

[17] Mindaugas Civilka, Lina Šlapimaitė, *Asmens duomenų samprata elektroninėje erdvėje*. (TEISĖ, 2015). Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/download/8761/7647/, 130 psl.
[18] Darius Štitilis, Mindaugas Kiškis, Tadas Limba, *„Interneto ir technologijų teisė“*. (Vilnius: Registrų centras, 2016), 331 psl.
[19] Europos Komisija, *Nuomonė 05/2014 dėl nuasmeninimo metodų*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 12 psl.
[20] Europos Komisija, *„Apie asmens duomenų apsaugos reformą“*. Žiūrėta 2019 rugsėjo 17. Prieiga per internetą: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_lt .
[21] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 92 psl.
[22] *Ibid*, 92 psl.
[23] *Ibid*, 92-95 psl.

nereiškia, kad ji nėra asmens duomenys“[24]. 2012 m. Lietuvos Vyriausiasis Admnistracinis teismas (toliau – LVAT) pripažino, kad tokie duomenys kaip automobilio valstybinis numeris, automobilio modelis, automobilio pagaminimo metai laikytini asmens duomenimis[25]. Panašiai ir 2014 m. Vilniaus miesto apylinkės teismo byloje, kuomet telefono numeris buvo taip pat pripažintas asmens duomenimis[26]. EK Nuomonėje 4/2007 nurodoma, jog „iš esmės duomenų apsaugos taisyklės jau numato galimybę, kad informacija gali būti neteisinga ir suteikia duomenų subjektui teisę susipažinti su informacija bei ją užginčyti naudojantis atitinkamomis priemonėmis“[27]. „Kalbant apie informacijos formatą arba laikmeną, asmens duomenų sąvoka apima informaciją bet kokia forma, neatsižvelgiant į tai, kaip ji pateikiama – raidėmis, skaičiais, grafiniu, fotografiniu vaizdu ar garso forma. Tai gali būti rašytinė informacija, taip pat kompiuterio atmintyje saugoma informacija, įvesta naudojant dvejetainį kodą[28], arba, pavyzdžiui, į vaizdajuostę įrašyta informacija. Tai yra loginis automatinio asmens duomenų tvarkymo įtraukimo į jos taikymo sritį padarinys. Šiuo atžvilgiu garsiniai ir vaizdiniai duomenys yra asmens duomenys visų pirma todėl, kad jie gali suteikti informacijos apie asmenį“[29]. Pavyzdžiui, pasak Valstybinę duomenų apsaugos inspekciją interneto protokolo (IP) adresas (unikalus numeris, identifikuojantis prisijungimo prie elektroninių ryšių tinklo įrenginį), atsižvelgiant į tai, kad yra susietas su konkrečiu asmeniu, taip pat daugelių atvejų laikytinas asmens duomenimis[30]. Pažymėtina, kad IP adresas buvo pripažintas asmens duomenimis ir 2016 m. spalio 19 d. sprendime Breyer[31]. Taigi, pirmas elementas nurodo, jog iš esmės bet kokia ir bet kokiu pavidalu išreikšta informacija gali būti laikoma asmens duomenimis, nepaisant to ar tai nuomonė ar faktas, ar tokia informacija atitinka tikrovę ar ne. Tokiu atveju vien pirmo elemento, dėl jo plataus interpretavimo, nepakaktų nustatyti ar atitinkama informacija yra asmens duomenys, ar ne.

Kitas elementas yra – informacijos sąsajumas su asmeniu. Remiantis minėta monografija, informacijos sąsajumas reiškia, jog atitinkama informacija yra apie tą konkretų asmenį[32]. Julius Zaleskis rašė: „duomenys yra susiję su asmeniu, jeigu jie nurodo asmens tapatybę, ypatybes ar elgesį arba jei tokia informacija naudojama siekiant nustatyti, kaip elgiamasi su tuo

---

[24] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 92 psl.
[25] „Lietuvos vyriausiojo administracinio teismo nutartis 2012 m. liepos 26 d. administracinioje byloje Nr. A-858-2133-12“, Liteko: http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=8220958e-b311-4bf4-ba16-980112510ccb
[26] „Vilniaus miesto apylinkės teismo nutarimas 2014 m. vasario 26 d. administracinio teisės pažeidimo byloje Nr. A2.11.-1793-295/2014“, E-teismai: https://eteismai.lt/byla/59726336888973/A2_11_-1793-295/2014
[27] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 6 psl.
[28] *Kodas, kuriam užrašyti vartojami du ženklai, paprastai 0 ir 1.*
[29] Europos Komisija, *op.cit.,* 7 psl.
[30] Valstybinė duomenų apsaugos inspekcija, *„Ar IP adresas yra asmens duomenys?“*, 2015 gegužės 25 d. Prieiga per internetą: https://www.ada.lt/go.php/lit/1-ar-ip-adresas-yra-asmens-duomenys-2014-m
[31] „Europos Sąjungos Teisingumo teismo sprendimas 2016 m. spalio 19 d. byloje Breyer Nr. C-582/14“. Eur-lex: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62014CJ0582&from=FR
[32] Zaleskis, *op.cit.*, 93 psl.

asmeniu arba kaip jis vertinamas, arba daryti jam poveikį“[33]. „Kai kuriais atvejais iš duomenų gaunama informacija pirmiausia yra susijusi su objektais, o ne su asmenimis. Tie objektai paprastai kam nors priklauso, jiems asmenys gali daryti tam tikrą poveikį arba jie gali daryti tam tikrą poveikį asmenims, taip pat objektai gali būti fizine ar geografine prasme artimi asmenims arba kitiems objektams. Tokiais atvejais galima laikyti, kad informacija su tais asmenimis arba objektais susijusi netiesiogiai“[34]. Pavyzdžiui namas, viena vertus informacija apie jį gali būti naudojama nurodant konkretaus rajono nekilnojamo turto kainų lygį, kita vertus – tokio namo vertė gali būti naudojama siekiant įvertinti konkretaus asmens potencialią galimybę mokėti mokesčius[35]. Taip pat kitas pavyzdys – palydovinė vietos nustatymo sistema, įdiegta taksi automobiliuose. Tokia sistema leidžia ne tik nustatyti kurioje vietoje yra atitinkamas taksi automobilis, bet ir padeda įvertinti taksi vairuotojo darbo kokybę, ar jis nenusižengia greičio ribojimams, ar atitinkamu metu buvo taksi automobilyje ar ne ir t.t.[36]. Pastaruoju atveju tokia informacija apie vairuotoją bus laikoma susijusi su asmeniu, nes ji atskleidžia apie jį detalius duomenis, taip pat gali charakterizuoti asmenį kaip darbuotoją. „Diskusijose apie duomenų apsaugą, kilusiose dėl RDA[37] *(radijo dažninio atpažinimo – aut.)* žymenų, darbo grupė pažymėjo, kad „duomenys yra susiję su asmeniu, jeigu jie nurodo asmens tapatybę, ypatybes ar elgesį arba jei tokia informacija naudojama siekiant nustatyti, kaip elgiamasi su tuo asmeniu arba kaip jis vertinamas, arba daryti susijusį poveikį““[38]. Kitaip tariant sąsajumas su konkrečiu asmeniu egzistuoja tuo atveju, jeigu remiantis atitinkamais duomenimis galima tokį asmenį identifikuoti, apibūdinti, nustatyti jo tam tikrus požymius ir pan.

Trečias elementas – fizinio asmens samprata. „Duomenų apsaugos teise užtikrinama apsauga turėtų būti taikoma fiziniams asmenims tvarkant jų asmens duomenis [...]. Ši apsauga neapima juridinių asmenų ir visų pirma juridinio asmens statusą turinčių įmonių duomenų, įskaitant juridinio asmens pavadinimą, teisinę formą ir kontaktinius duomenis, tvarkymo (BDAR preambulės 14 p.)“[39]. Grįžtant prie anksčiau aptartos Europos Komisijos asmens duomenų sąvokos, buvo nustatyta, kad toks fizinis asmuo, be kita ko turi būti ir gyvas[40]. Paaiškinimas kodėl taip yra, pateikia Europos Komisija: „valstybių narių teisės aktuose, paprastai civilinėje teisėje, tiksliau nusakoma

---

[33] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 93 psl.
[34] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 9 psl.
[35] *Ibid*, 9 psl.
[36] *Ibid*, 11 psl.
[37] *RDA — tai technologija, pagrįsta automatiniu atpažinimu ir duomenų išgava naudojant radijo dažnius. Pagrindiniai šios technologijos požymiai — galimybė naudojant elektroninį žymenį prie bet kokio objekto, gyvūno ar net žmogaus pritvirtinti unikalų identifikatorių arba kitokią informaciją ir naudojantis bevieliu prietaisu skaityti šią informaciją.*
[38] Europos Komisija, *op.cit.*, 10 psl. Cituota iš 2005 m. sausio 19 d. darbo grupės dokumentas Nr. WP 105 „Darbo dokumentas dėl duomenų apsaugos klausimų, susijusių su RDA technologija“, 8 psl.
[39] Zaleskis, *op.cit.*, 93 psl.
[40] Europos Komisija, *„Apie asmens duomenų apsaugos reformą“.* Žiūrėta 2019 rugsėjo 17. Prieiga per internetą: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_lt .

žmogaus asmenybės sąvoka, kuri suprantama kaip gebėjimas būti teisinių santykių subjektu nuo asmens gimimo iki jo mirties. Todėl asmens duomenys iš esmės yra susiję su gyvais asmenimis, kurių tapatybė nustatyta arba gali būti nustatyta, susiję duomenys“[41]. Panašu, kad tokios pozicijos laikomasi ir Lietuvoje, nes asmens civilinis teisnumas (galėjimas turėti civilinės teises ir pareigas) remiantis CK 2.2 str. 1 d. atsiranda asmens gimimo momentu ir išnyksta jam mirus[42]. Tačiau EK dar pabrėžia, kad tam tikrais atvejais ir mirusiųjų asmenų duomenims gali būti taikoma asmens duomenų teisinė apsauga. Pavyzdžiui toks atvejis, kai miręs asmuo sirgo genetiškai perduodama liga atskleidžia informaciją, kad tokio asmens vaikai taip pat gali susirgti šia liga, tokiu būdu informacija apie mirusįjį asmenį netiesiogiai gali atskleisti ir kitų gyvų asmenų duomenis, šiuo atveju duomenis apie sveikatą[43]. Kalbant apie juridinių asmenų duomenis, jiems taip pat tam tikrais atvejais gali būti taikomos išimtis. „Informacija apie juridinius asmenis taip pat gali būti laikoma iš esmės susijusia su fiziniais asmenimis. Taip gali būti tada, kai juridinio asmens pavadinimas susijęs su fizinio asmens vardu ar pavarde. Kitas pavyzdys būtų kolektyvinis elektroninio pašto adresas, kuriuo paprastai naudojasi konkretus darbuotojas, arba informacija apie mažą įmonę (teisiškai kalbant veikiau „objektą“ negu juridinį asmenį), pagal kurią galima apibūdinti savininko elgesį. Visais tais atvejais, kai turinio, tikslo ar rezultato kriterijai leidžia informaciją apie juridinį asmenį ar įmonę laikyti susijusia su fiziniu asmeniu, tokią informaciją reikia laikyti asmens duomenimis ir taikyti duomenų apsaugos taisykles“[44]. Taigi, paprastai asmens duomenų apsauga yra taikoma gyviems fiziniams asmenims, tačiau išskirtiniais atvejais gali pasitaikyti ir išimčių.

Ir ketvirtas elementas – galimybė nustatyti tapatybę. Pasak monografijos autorių: „reikėtų atsižvelgti į visas priemones, kurias iš jų tiesiogiai ar netiesiogiai nustatant asmens tapatybę, tikėtina, pagrįstai galėtų naudoti duomenų valdytojas ar kitas asmuo[45]. „Tapatybė paprastai nustatoma pagal konkrečią informaciją, kurią galima vadinti „žymenimis tapatybei nustatyti“ ir kuri yra labai išskirtinai ir glaudžiai susijusi su konkrečiu asmeniu. Tai gali būti to asmens išvaizdos požymiai, pavyzdžiui, ūgis, plaukų spalva, apranga ir kt., arba asmens ypatybė, apie kurią neįmanoma sužinoti iš karto, pavyzdžiui, profesija, pareigos, vardas bei pavardė ir kt.“[46]. Kaip jau buvo minėta anksčiau, asmens tapatybė gali būti nustatyta tiek tiesiogiai, tiek netiesiogiai. Tuo atveju, kai asmens tapatybė yra arba gali būti nustatyta tiesiogiai, paprastai asmuo identifikuojamas pagal įprastus

---

[41] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 21 psl.
[42] „Lietuvos Respublikos civilinis kodeksas*“, Valstybės žinios*, (2000).
[43] Europos Komisija, *op.cit.,* 21-22 psl.
[44] *Ibid*, 23 psl.
[45] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 95 psl.
[46] Europos Komisija, *op.cit.,* 12 psl.

identifikatorius, tokius kaip vardas, pavardė, ir tai yra paprasčiausias žymuo tapatybei nustatyti[47]. Prie jo taip pat galima jungti ir kitus žymenis (gimimo data, nuotrauka ir pan.), siekiant tiksliai nustatyti asmens tapatybę; pagrindinis kriterijus tokiu atveju būtų – ar galima vieną asmenį pagal turimus duomenis išskirti iš kitų[48]. „Kalbant apie asmenis, kurių tapatybė yra arba gali būti nustatyta netiesiogiai, ši kategorija paprastai susijusi su mažos arba didelės apimties unikalių junginių reiškiniu. Kai prima facie turimų žymenų tapatybei nustatyti nepakanka konkrečiam asmeniui išskirti, to asmens tapatybę vis dėlto galima nustatyti, nes sudėjus tuos duomenis su kita informacija (neatsižvelgiant į tai, ar duomenų valdytojas ją turi) bus įmanoma išskirti tą asmenį iš kitų“[49]. Pavyzdys iš praktikos: Europos Sąjungos Teisingumo Teismas (toliau – ESTT) 2017 m. gruodžio 20 d. byloje Peter Nowak buvo pasisakęs dėl egzaminuojamojo profesinio egzamino metu pateiktų raštiškų atsakymų ir taip pat dėl egzaminuotojo dėl šių atsakymų pateiktos pastabos – ar tai atitinka asmens duomenų sąvokos duomenų apsaugos prasme[50]. „P. Nowak keturis kartus neišlaikė egzamino. Ketvirtąjį kartą neišlaikęs egzamino, P. Nowak pateikė prašymą leisti susipažinti su juo tvarkomais asmens duomenimis. Licencijuotų apskaitininkų institutas atsisakė jam pateikti jo egzamino darbo kopiją, nes jame nebuvo asmens duomenų, kaip tai suprantama pagal Asmens duomenų apsaugos įstatymą. Tuomet P. Nowak kreipėsi į Duomenų apsaugos komisarą, vėliau į teismą. Teismas nurodė, kad [...] profesinį egzaminą laikantis asmuo yra fizinis asmuo, kuris gali būti nustatytas arba tiesiogiai, remiantis jo vardu ir pavarde, arba netiesiogiai, pagal jo identifikacinį numerį, kurie nurodyti ant egzamino darbo kopijos arba ant šios kopijos viršelio. Neturi reikšmės tai, ar egzaminuotojas taisydamas ar vertindamas egzamino darbo kopiją gali identifikuoti egzaminuojamąjį. Tam, kad duomenys galėtų būti laikomi asmens duomenimis nereikalaujama, kad visa informacija, leidžianti identifikuoti atitinkamą asmenį, būtų prieinama vienam ir tam pačiam asmeniui. Tuo atveju, kai egzaminuotojas vertindamas egzaminuojamojo egzamino metu pateiktus atsakymus nežino jo tapatybės, egzaminą organizuojantis subjektas, šiuo atveju licencijuotų apskaitininkų institutas, disponuoja būtina informacija, leidžiančia jam lengvai ir aiškiai identifikuoti šį egzaminuojamąjį pagal jo ant egzamino darbo kopijos arba šios kopijos viršelio nurodytą identifikacinį numerį, ir taip priskirti jam atsakymus“[51]. Vadinasi, net ir tuo atveju, kai turima dalis informacijos apie konkretų asmenį jo tiesiogiai dar neidentifikuoja, tačiau esant galimybei tokią

[47] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 12 psl.
[48] *Ibid*, 12 psl.
[49] *Ibid*, 13 psl.
[50] „Europos Sąjungos Teisingumo Teismo sprendimas 2017 m. gruodžio 20 d. byloje Peter Nowak Nr. C-434/16“, Europos Sąjungos Teisingumo Teismo praktikos apžvalga: https://www.lat.lt/data/public/uploads/2018/03/estt_2017_gruodis.pdf, 13 psl.
[51] *Ibid*, 13-14 psl.

informaciją sujungti su kita, net ir esančią pas kitą asmenį, pagal kurią bus galima asmenį identifikuoti reiškia, kad tokio asmens tapatybė gali būti nustatyta.

Apibendrinant pateiktą informaciją daroma išvada, jog asmens duomenų samprata yra ganėtinai plati, ji apima iš esmės bet kokią informaciją turinčią šiuos tarpusavyje susijusius elementus: informacijos samprata, informacijos sąsajumas su asmeniu, fizinio asmens samprata ir galimybė nustatyti tapatybę. Ar atitinkama informacija atitinka asmens duomenų sampratą ar ne, reikėtų vertinti kiekvienu konkrečiu atveju, nes ta pati informacija skirtingais atvejais gali būti laikoma asmens duomenims arba ne. Taigi atsižvelgiant į nustatytus asmens duomenų sampratos elementus, bendrai asmens duomenis galima apibūdinti taip – tai objektyvi ir (arba) subjektyvi informacija, kuri apibūdina, nustato, charakterizuoja, atskleidžia atitinkamus požymius arba kitaip tiesiogiai ar netiesiogiai identifikuoja fizinį gyvą asmenį, neatsižvelgiant į tai, ar tokią informaciją turi vienas asmuo, ar ši informacija egzistuoja pas kelis skirtingus asmenis.

1.2. Anoniminiai duomenys

Atsižvelgiant į tai, kad Bendrojo duomenų apsaugos reglamento preambulėje pasakytina, jog anoniminiai informacijai nėra taikomi asmens duomenų apsaugos principai, taip pat į tai, kad anoniminiai duomenys iš esmės yra anonimizavimo proceso rezultatas[52], yra svarbu nustatyti anonominių duomenų sampratą, atriboti juos nuo asmens duomenų bei nustatyti aiškų šių duomenų santykį asmens duomenų anonimizavimo prasme.

Bendrasis duomenų apsaugos reglamentas anoniminius duomenis apibrėžia kaip „informaciją, kuri nėra susijusi su fiziniu asmeniu, kurio tapatybė nustatyta arba gali būti nustatyta, arba asmens duomenims, kurių anonimiškumas užtikrintas taip, kad duomenų subjekto tapatybė negali arba nebegali būti nustatyta“. Analizuojant šį apibrėžimą galima daryti išvadą, kad BDAR nurodo, jog anonominiai duomenys gali būti dviejų rūšių. Pirma rūšys – tai yra tam tikra informacija, kuri ir be specialaus apdorojimo nenustato konkretaus asmens tapatybes, kitaip tariant tai gali būti neutrali, iš prigimties su fiziniu asmeniu nesusijusi informacija. Ir antra rūšys, kuri yra ypač aktuali šio darbo tyrimui, tai po specialaus apdorojimo asmens duomenys, kurie po tokio apdorojimo neteko tam tikrų asmens duomenims būdingų elementų, ko pasekoje prarado galimybę identifikuoti tam tikrą asmenį ir tapo anoniminiais. „Big Data – Algorithms, Analytics, and Applications“ knygos autoriai anoniminius duomenis apibrėžia panašiai: tai yra duomenys, kurie nebegali būti tiesiogiai ar netiesiogiai susieti su identifikuotu arba identifikuojamu asmeniu originaliai arba po apdorojimo[53].

[52] Deryck Beyleveld ir kt., *„The Data Protection Directive and Medical Research Across Europe“,* (Taylor & Francis, 2017), 38 psl.
[53] Kuan-Ching Li ir kt., *„Big Data – Algorithms, Analytics, and Applications“*, (CRC Press, 2015), 293 psl.

Pabrėžtina, kad ir šie autoriai akcentuoja, jog duomenys gali būti anoniminiai iš prigimties arba po apdorojimo. Remiantis Europos Komisijos pateikta nuomone, anoniminiai duomenys – tai bet kokia informacija susijusi su fiziniu asmeniu, kai asmens tapatybės negali nustatyti nei duomenų valdytojas, nei bet koks kitas asmuo, atsižvelgiant į visas priemones, kuriomis galėtų pasinaudoti duomenų valdytojas ar bet kuris kitas asmuo asmens tapatybei nustatyti[54]. Autorius pastebi, kad šiuo atveju dar atkreipiamas dėmesys į tai, kad iš anoniminių duomenų, net ir panaudojus kitą papildomą informaciją arba priemones, neturi būti nustatoma tam tikro asmens tapatybė. Kiti autoriai pabrėžia, kad anoniminiai duomenys laikomi tie duomenys, kurių duomenų subjekto tapatybė nežinoma ir negali būti identifikuojama, nes surinkus informaciją pagal kurią buvo galima asmenį identifikuoti, vėliau ji buvo anonimizuota[55]. Taigi sistemiškai vertintant visus šiuos apibrėžimus galima išskirti tam tikrus anoniminių duomenų požymius, tai yra 1) tam tikra informacija, 2) kuri yra susijusi su atitinkamu asmeniu ir 3) pagal ją neįmanoma arba nebeįmanoma tiesiogiai arba netiesiogiai nustatyti asmens tapatybes.

Europos Komisijos gairėse dėl Reglamento dėl laisvo ne asmens duomenų judėjimo nurodyta: „jei duomenys nėra Bendrajame duomenų apsaugos reglamente apibrėžti kaip asmens duomenys, jie laikomi ne asmens duomenimis. Pagal kilmę galima išskirti šias ne asmens duomenų grupes: pirma, duomenys, kurie nuo pat pradžių nėra susiję su fiziniu asmeniu, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti, pavyzdžiui, ant vėjo jėgainių įrengtų jutiklių sugeneruoti duomenys apie oro sąlygas arba duomenys apie pramonės mašinų techninės priežiūros poreikius; antra, duomenys, kurie iš pradžių buvo asmens duomenys, bet vėliau tapo anoniminiai“[56]. Pirmiausia šiuo apibrėžimu pabrėžiamas jau anksčiau minėtas anoniminių duomenų išskyrimas į iš prigimties esančią anoniminę informaciją ir į anonimizuotus duomenis. Be to, pateikiamas ir anoniminių duomenų apibrėžimas, šiuo atveju anoniminiai duomenys apibrėžiami kaip ne asmens duomenys ir teigiama, kad viskas kas nepatenka į asmens duomenų sampratą laikoma ne asmens duomenimis. Autoriaus manymu, reikia turėti omenyje, kad ne asmens duomenų samprata yra ganėtinai plati ir apima ne tik anoniminius duomenis, bet ir kitus duomenis, kaip pavyzdžiui aukščiau aptartus juridinių asmenų duomenis, mirusiųjų asmenų duomenis ir kitus duomenis, kurie neatitinka asmens duomenų sampratos duomenų apsaugos teisės prasme, bet tuo pačiu nėra ir anoniminiai. Reglamentas dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų pateikia ne asmens duomenų pavyzdinį sąrašą: tai yra „suvestiniai ir anonimizuoti duomenų rinkiniai, naudojami

---

[54] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 20 psl.

[55] Deryck Beyleveld ir kt., *„The Data Protection Directive and Medical Research Across Europe“,* (Taylor & Francis, 2017), 147 psl.

[56] Komisijos Komunikatas Europos Parlamentui ir Tarybai, *„Gairės dėl Reglamento dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“*, 2019 gegužės 29 d. Eur-lex: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2019:250:FIN

didžiųjų duomenų analizei, duomenys apie tikslųjį ūkininkavimą, kurie gali padėti stebėti ir optimizuoti pesticidų ir vandens naudojimą, arba duomenys apie pramonės mašinų techninės priežiūros poreikius“[57]. Kaip matoma iš šio pavyzdžio, anonimizuoti duomenys yra tik vieni iš ne asmens duomenų.

Visuomenėje egzistuoja nuomonė, kad visiškai ir negrįžtamai anonimizuotų duomenų nėra[58]. Reglamentas dėl laisvo ne asmens duomenų judėjimo taip pat nurodo, kad „jei dėl technologijų pokyčių anonimizuotus duomenis tampa įmanoma paversti asmens duomenimis, tokie duomenys turi būti laikomi asmens duomenimis ir atitinkamai turi būti taikomas Reglamentas (ES) 2016/679“. Londono „Imperial“ koledžo ir Katalikų Universiteto de Louvaino (Belgija) mokslininkai žurnale „Nature Communications“ pranešė sukūrę kompiuterio algoritmą, pagal kurį galima nustatyti 99,98 proc. amerikiečių iš beveik bet kokio turimo duomenų rinkinio, turinčio tik 15 požymių, tokių kaip lytis, pašto kodas ar šeimyninė padėtis ir pan.[59]. Taip pat praktikoje pasitaikė atvejų, kai asmens duomenys buvo deanonimizuoti, kitaip tariant atskleisti; vienas tokių atvejų buvo 2008 metais, kai anonimizuotas „Netflix“ filmų reitingų duomenų rinkinys buvo deanonimizuotas palyginus reitingus su viešais balais „IMDb“ filmų svetainėje 2014 metais, taip pat kitas pavyzdys – Niujorko taksi vairuotojų namų adresai buvo atskleisti iš anoniminių duomenų apie individualias keliones mieste ir kt.[60]. Atsižvelgiant į tai Europos Komisija pabrėžia, kad „tik tuo atveju, kai duomenų valdytojas duomenis agreguoja tokiu lygmeniu, kuriuo nebegalima nustatyti individualių įvykių, iš tokių duomenų sudarytas duomenų rinkinys gali būti laikomas anoniminiu. Pavyzdžiui, jeigu organizacija įvykių lygmeniu renka duomenis apie asmenų judėjimą kelionių metu, įvykių lygmens duomenys apie asmenų keliavimo būdą bet kurios šalies požiūriu vis dar bus laikomi asmens duomenimis, jeigu duomenų valdytojas (arba bet kuri kita šalis) tebeturės galimybę gauti pirminius netvarkytus duomenis, net jeigu iš trečiosioms šalims pateikto rinkinio buvo pašalinti tiesioginiai identifikatoriai. Bet jeigu duomenų valdytojas ištrintų netvarkytus duomenis ir trečiosioms šalims pateiktų tik aukštu lygmeniu agreguotus statistikos duomenis, pvz., X kryptimi pirmadieniais važiuoja 160 proc. daugiau keleivių nei antradieniais, tai būtų laikoma anoniminiais duomenimis“[61]. Taigi, pašalinus asmens duomenų identifikatorius iš viešosios erdvės, dar nereiškia, kad tokie duomenys tapo anoniminiais,

---

[57] „Europos Parlamento ir Tarybos reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“, *Europos Sąjungos leidinys*, (2018).

[58] *„Anonymised' data can never be totally anonymous, says study“*, žiūrėta 2019 spalio 19 d. Prieiga per internetą: https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds

[59] Gina Kolata, *„Your Data Were 'Anonymized'? These Scientists Can Still Identify You“*, (NY times: 2019 liepos 23 d.) Prieiga per internetą: https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html

[60] *„Anonymised' data can never be totally anonymous, says study“*, žiūrėta 2019 spalio 19 d. Prieiga per internetą: https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds

[61] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 9-10 psl.

ypač tuo atveju, kai tokie identifikatoriai yra saugomi pas duomenų valdytoją ar kitą už duomenų saugojimą atsakingą asmenį.

Tiek Bendrajame duomenų apsaugos reglamente, tiek Reglamente dėl laisvo ne asmens duomenų judėjimo pabrėžiamas anoniminių duomenų ypatumas – jie iš pat pradžių buvo susieti su konkrečiu asmeniu, tačiau po atitinkamo apdorojimo, t.y. anonimizavimo, tapo anoniminiais. Europos Komisija pasisakydama dėl asmens duomenų anonimizavimo, pažymėjo, kad tai yra tolesnis asmens duomenų tvarkymas ir jis turi būti vykdomas atsižvelgiant į teisinį pagrindą ir tolesnio tvarkymo aplinkybes[62]. Šiuo atveju tolesnis asmens duomenų tvarkymas reiškia, kad „pradinė sąlyga yra ta, kad asmens duomenys turėjo būti renkami ir tvarkomi remiantis taikomais teisės aktais dėl duomenų laikymo ir būti tokio pavidalo, kad būtų galima nustatyti asmens tapatybę“[63]. Autoriaus manymu, tokiu būdu atsiranda santykis su asmens duomenimis. Tai reiškia tam, kad atitinkami anoniminiai duomenys būtų naudojami tam tikru tikslu, pavyzdžiui statistiniais tikslais ar istorinių tyrimų tikslais, iš pat pradžių buvo renkami asmens duomenys, kurie buvo susieti su konkrečiu asmeniu, kurio tapatybę buvo įmanoma nustatyti ir tt. Be kita ko, jie turėjo būti renkami remiantis duomenų apsaugos teisę reglamentuojančių teisės aktų reikalavimų, pvz. turint teisėtą pagrindą ir tikslą, tačiau vėliau tikslui pasiekti asmens tapatybės nustatymas ir kiti asmens duomenims būdingi elementai tapo nebereikalingi, todėl siekiant apsaugoti duomenų subjektą nuo galimos grėsmės bei atitikti duomenų apsaugos reikalavimus, duomenys buvo apdoroti tokiu būdu, kad buvo panaikinta galimybė nustatyti konkretaus asmens tapatybę, kitaip tariant duomenys tapo anoniminiais.

Autorius atkreipia dėmesį, jog asmens duomenys ir anoniminiai duomenys nėra tas pats, todėl yra svarbu atriboti asmens duomenis nuo anoniminių duomenų. Atribojant šiuos duomenys vienus nuo kitų, svarbus aspektas yra sąsaja su konkrečiu asmeniu. Apie sąsają su konkrečiu asmeniu plačiau buvo kalbama 1.1. skyriuje, kai buvo aptariami asmens duomenų sampratos elementai. Europos Komisijos gairėse dėl laisvo ne asmens duomenų judėjimo teigiama: „jei ne asmens duomenis galima kokiu nors būdu susieti su konkrečiu asmeniu ir taip sudaryti sąlygas tiesiogiai ar netiesiogiai nustatyti jo tapatybę, šie duomenys turi būti laikomi asmens duomenimis. Pavyzdžiui, jei gamybos linijos kokybės kontrolės ataskaitos duomenis galima susieti su konkrečiais gamyklos darbuotojais (pavyzdžiui, darbuotojais, kurie nustato gamybos parametrus), jie turi būti laikomi asmens duomenimis ir turi būti taikomas Bendrasis duomenų apsaugos reglamentas. Tokios pačios taisyklės taikomos, kai dėl technologijų ir duomenų analizės raidos tampa įmanoma anoniminius

---

[62] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 3 psl.
[63] *Ibid*, 7 psl.

duomenis paversti asmens duomenimis“[64]. Kitas pavyzdys – viešai paskelbta žmogaus nuotrauka su užtušuotų veidu, viena vertus nepažįstamiems asmenims tokio asmens tapatybė nebus žinoma ir jo atpažinti tikėtina negalės, kita vertus kiti žmonės, kurie gerai pažįsta asmenį iš nuotraukos, gali jį atpažinti ir iš kitų kūno vietų, savybių, laikysėnos, aprangos ir pan[65]. Pastarasis atvejis rodo, kad nors ir ne visiems asmenims yra galimybė susieti aptarta nuotrauka su konkrečiu asmeniu, tačiau tam tikrai daliai žmonių tokia galimybė egzistuoja, reiškia, jog šiuo atveju yra sąsaja su konkrečiu asmeniu, vadinasi tai būtų asmens duomenys, o ne anoniminiai duomenys. Taigi norint atriboti anoniminius duomenis nuo asmens duomenų, pirmiausia reikia atsižvelgti į tai, ar atitinkama informacija turi ryšį su tam tikru asmeniu ir ar remiantis ja būtų galima tokį asmenį identifikuoti, taip pat vertėtų atsižvelgti ar neegzistuoja kitų asmens duomenų sampratos elementų, kurie jau buvo anksčiau aptarti šiame darbe.

Kalbant apie anoniminių duomenų teisinę apsaugą, svarbu dar kartą pabrėžti, kad anoniminiai informacijai nėra taikomi asmens duomenų apsaugą reglamentuojantys teisės aktai ir principai. Taip pat remiantis iki BDAR įsigaliojimo taikoma Direktyva 95/46/EB duomenims[66], kurie paversti anoniminiais, taip pat nebuvo taikomi duomenų apsaugos teisės aktai. Tačiau tai nereiškia, kad tokiems duomenims nėra taikoma jokia apsauga. Atsižvelgiant į Europos Komisijos aiškinimą, ne asmens duomenims, tame tarpe ir anoniminiams duomenims taikomi kiti nei asmens duomenų apsaugai taikomi teisės aktai, pavyzdžiui 2018 m. lapkričio 14 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų, taip pat tokiems duomenims apsaugoti gali būti pasirašomi konfidencialumo įsipareigojimai ir kt.[67]. Autorius manymu, aplinkybė, jog anoniminiai informacijai nėra taikomi griežti asmens duomenų apsaugos reikalavimai, gali būti priežastis kodėl duomenų valdytojui gali būti naudinga naudoti būtent anoniminius duomenis savo tikslams pasiekti.

Apibendrinant galima daryti išvadą, kad anoniminiai duomenys yra duomenys, kurie nenustato asmens tapatybės, taip pat pagal juos neįmanoma atitinkamą asmenį identifikuoti bei nustatyti jo požymius. Taip pat išsiaiškinta, kad anoniminiai duomenys gali būti dviejų rūšių, t.y. 1) jie gali būti anoniminiai pagal savo prigimtį arba 2) specialiai anonimizuoti. Iš to seka išvada, kad duomenys, kurie nėra anonimiški iš prigimties, o tapo tokiais tik asmens duomenų anonimizavimo rezultate, turi neabejotiną ryšį su asmens duomenimis. Toks ryšys pasireiškia tuo atveju, kai asmens

---

[64] Komisijos Komunikatas Europos Parlamentui ir Tarybai, *„Gairės dėl Reglamento dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“*, 2019 gegužės 29 d. Eur-lex: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2019:250:FIN

[65] Europos Komisija, *„Nuomonė 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf, 21 psl.

[66] „Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, *Europos Sąjungos oficialusis leidinys*, (1995).

[67] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 3 psl.

duomenys po specialaus apdorojimo praranda savo būtiniausius elementus, kurie buvo aptarti 1.1. skyriuje, ko pasekoje eliminuojama galimybė susieti duomenis su konkrečiu asmeniu ir nustatyti jo tapatybę. Tokioje situacijoje duomenys laikomi anoniminiais asmens duomenų anonimizavimo proceso prasme ir jiems nustoja galioti asmens duomenų apsaugai taikomi teisės aktai.

1.3. Asmens duomenų anonimizavimo samprata

BDAR preambulės 156 straipsnyje yra numatyta, kad tvarkant asmens duomenis viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, jie turi būti tvarkomi taip, kad siekiant minėtų tikslų būtų užtikrintos tokios duomenų saugumo priemonės, kurios neleistų nustatyti atitinkamo duomenų subjekto tapatybės. Kaip jau buvo išsiaiškinta anksčiau, asmens tapatybės nustatymas yra negalimas tuo atveju, kai duomenys yra anoniminiai. Taip pat ir iš anonimizuotų duomenų, duomenų subjektui neturi kilti gresmė, kad jo tapatybė bus nustatyta ir (ar) atskleista. Vis dėl to svarbu aiškiai apibrėžti kas yra asmens duomenų anonimizavimas, todėl toliau bus nustatoma jo samprata.

Kaip jau buvo minėta, nei Bendrasis duomenų apsaugos reglamentas, nei LR asmens duomenų teisinės apsaugos įstatymas tiesiogiai neįtvirtina asmens duomenų anonimizavimo sąvokos. Tačiau asmens duomenų anonimizavimo apibrėžimą galima rasti doktrinoje. Pavyzdžiui, „The Complete Book of Data Anonymization – From Planning to Implementation“ autoriaus teigimu, anonimizavimas tai procesas, kuriuo metu nuasmeninama jautri informacija (asmens duomenys) išsaugant jos formatą ir duomenų tipą[68]. Taip pat anonimizavimas apibrėžiamas ir kaip procesas, kuriuo metu asmens duomenys pakeičiami tokia forma, kad asmens tapatybė nebegali būti nustatoma[69]. Dar teigiama, kad anonimizavimas nutraukia ryšį tarp atitinkamų duomenų ir duomenų subjekto[70]. Visiškas anonimizavimas reiškia, kad duomenys daugiau nebegali būti sujungiami su asmenimis ir iš jų negrįžtamai pašalinami visi identifikatoriai[71]. Remiantis Europos Komisijos nuomone, duomenys laikomi nuasmeninti tuo atveju, kai iš jų yra pašalinami visi elementai, kurie leidžia nustatyti asmens tapatybę[72]. Atsižvelgiant į išdėstytas sąvokas, autorius daro išvadą, kad ko gero vieningą asmens duomenų anonomizavimo sąvoką būtų sudėtingą rasti, ji interpretuojama

---

[68] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf, 4 psl.
[69] Kristel Toom, Pamela F. Miller, *„Research Management“*, (Academic Press, 2018). Prieiga per internetą: https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/anonymization
[70] Catherine Tessier, Vincent Bonnemains, *„Neuroergonomics“*, (Academic Press, 2018), 67 psl.
[71] John C. Lindon, Jeremy K. Nicholson and Elaine Holmes, *„The Handbook of Metabolic Phenotyping“,* (Elsevier, 2019), 355 psl.
[72] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 5 psl.

skirtingai. Tačiau autorius pastebi, jog visi paminėti autoriai asmens duomenų anonimizavimą sieja su tam tikros informacijos pašalinimu ar pakeitimu, kuris pašalina tiesioginius ir netiesioginius identifikatorius bei kitus asmens duomenims būdingus elementus ir paverčia asmens duomenis anoniminiais.

Pažymėtina, kad nepaisant to, kad asmens duomenų anonimizavimas panaikina asmens tapatybės nustatymo galimybę, tokiu būdu apsaugant duomenis nuo galimų duomenų apsaugos pažeidimų, vis dėl to egzistuoja nuomone, kad asmens duomenų anonimizavimo metodų pagalba apdoroti duomenys nėra pats geriausiais ir patogiausiais sprendimas[73]. Londono universiteto koledžas pasisakydamas dėl asmens duomenų anonimizavimo pastebi, kad nors kai kurios organizacijos gali būti skatinamos tvarkyti duomenis anoniminiu pavidalu, ši metodika gali nuvertinti duomenis, todėl kai kuriais tikslais jie nebetenka naudos[74]. Autorius daro išvadą, kad iš tikrųjų vertinant kokia didelė apsauga yra taikoma asmens duomenims palyginus su anoniminiu duomenų apsauga, taip pat turint omenyje, kad asmens duomenims taikomas BDAR, kuris numato milžiniškas baudas už pažeidimus, o anoniminiams tokia apsauga ir sankcijos nėra taikomos, galima daryti išvadą, kad asmens duomenys yra kur kas vertingesni duomenų valdytojui, nes su jais jis tikėtina galėtų efektyviau pasiekti savo tikslų. Tačiau vis dėl to nereikėtų pamiršti, kad kaip jau buvo minėta, asmens duomenims palyginus su anoniminiais yra taikomi kur kas aukštesni duomenų apsaugos ir tvarkymo reikalavimai. Todėl nepaisant to, kad duomenų valdytojui asmens duomenis ir gali atrodyti vertingesni, siekiant sumažinti duomenų praradimo ir (ar) pažeidimo riziką, autorius mano, kad būtų saugiau naudotis būtent tomis duomenimis, kurie nekelia asmens identifikavimo rizikos, pavyzdžiui anoniminiais duomenimis.

Būtina atkreipti dėmesį, kad praktikoje pasitaiko ir netinkamo duomenų anonimizavimo taikymo pavyzdžių. Kaip antai 2018 m. spalio mėn. Danijos duomenų apsaugos institucija nustatė, kad Danijos taksi įmonė „Taxa“ saugo maždaug 9 milijonus taksi vairuotojų duomenis daugiau kaip penkerius metus po to, kai tokie duomenis tapo nebereikalingi[75]. Duomenų apsaugos inspekcijos patikrinimo metu buvo nustatyta, kad minėta taksi bendrovė be kita ko, netinkamai anonimizuoja asmens duomenis. Taksi bendrovė iš klientų sąrašų išbraukdavo asmens vardą ir pavardę, tačiau palikdavo asmeninį telefono numerį, pagal kurį taip pat galima asmenį identifikuoti, o anonimizavimas pasižymi tuo, kad negrįžtamai panaikina galimybę asmenį identifikuoti. Atsižvelgiant į tai duomenų apsaugos inspekcija nustatė, kad tokiu būdu nėra daromas realus asmens

---

[73] *„Anonymisation and Pseudonymisation of Personal data“*, žiūrėta 2019 rugsėjo 25 d. Prieiga per internetą: https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and#Anonymisation

[74] *Ibid*

[75] *„Data anonymization and GDPR compliance: the case of Taxa 4×35“*, žiūrėta 2019 spalio 27 d. Prieiga per internetą: https://gdpr.eu/data-anonymization-taxa-4x35/

duomenų anonimizavimas[76]. Galiausiai Danijos duomenų apsaugos inspekcija nurodė, kad toks įrašų saugojimas prieštarauja ES Bendrojo duomenų apsaugos reglamento 5 straipsniui, kuriame teigiama, kad asmens duomenys turi būti „adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi“ ir „laikomi tokia forma, kad duomenų subjektų tapatybę būtų galima nustatyti ne ilgiau, nei tai yra būtina tais tikslais, kuriais asmens duomenys yra tvarkomi“. Atsižvelgiant į tai, Danijos taksi įmonei gresia bauda už asmens duomenų apsaugos pažeidimą, kurios dydis gali siekti 160,000 eurų[77]. Autoriaus manymu, šis pavyzdys rodo, jog tik tinkamai pritaikytas asmens duomenų anonimizavimas gali užtikrinti visišką anonimiškumą. Taip pat autorius daro išvadą, kad netinkamai pritaikytas anonimizavimas gali būti priežastis, kodėl asmens duomenų anonimizavimas gali būti vertinamas kritiškai ir kodėl teigiama, kad jis negali užtikrinti duomenų subjektui anonimiškumo. Atsižvelgiant į tai, kad praktikoje pasitaiko netinkamo duomenų anonimizavimo pavyzdžių, tai skatina aiškiai apibrėžti asmens duomenų anonimizavimo procesą, siekiant išvengti galimų duomenų apsaugos pažeidimų.

Apibendrinant, asmens duomenų anonimizavimą galima apibrėžti kaip procesą, kuriuo metu asmens duomenys apdorojami tokiu būdu, kad iš jų būtų visiškai ir negrįžtamai pašalinami tiesioginiai ir netiesioginiai identifikatoriai bei kiti asmens duomenims būdingi elementai. Asmens duomenų anonimizavimo proceso rezultatas yra anoniminiai duomenys, kuriems, kaip jau buvo išsiaiškinta anksčiau, nėra taikomos asmens duomenų apsaugos taisyklės.

1.3.1. Anonimizavimo paskirtis

Nagrinėjant anonimizavimo sampratą, svarbus aspektas yra asmens duomenų anonimizavimo paskirtis. Kitaip tariant, kuo ši duomenų saugumo priemonė gali būti naudinga duomenų valdytojui ir (arba) duomenų subjektui.

Europos Komisijos asmenų apsaugos tvarkant asmens duomenis darbo grupė Nuomonėje 05/2014 dėl nuasmeninimo metodų (toliau – EK darbo grupė) pabrėžia, kad anonimizavimas gali būti vertingas tuo atveju, kai siekiama asmens duomenis panaudoti tiek pavienių asmenų, tiek visuomenės reikmėms ir tuo pačiu sumažinant gresiančius pavojus šių asmenų duomenų

[76] *„Supervision of Taxa 4x35's processing of personal data“*, (Datatilsynet, 2019 kovo 18 d.). Prieiga per internetą: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/tilsyn-med-taxa-4x35s-behandling-af-personoplysninger/

[77] *„Data anonymization and GDPR compliance: the case of Taxa 4×35“*, žiūrėta 2019 spalio 27 d. Prieiga per internetą: https://gdpr.eu/data-anonymization-taxa-4x35/

apsaugai[78]. „Kadangi naudojant įvairius įrenginius, jutiklius ir tinklus sukuriama gausybė duomenų ir atsiranda naujos duomenų rūšys, o duomenų laikymo kaina darosi nereikšminga, visuomenėje stiprėja kartotinio šių duomenų naudojimo interesas ir poreikis. Atvirieji duomenys visuomenei, pavieniams asmenims ir organizacijoms neabejotinai gali būti naudingi, tačiau tik tuo atveju, jeigu bus gerbiamos kiekvieno asmens teisės į asmens duomenų ir privataus gyvenimo apsaugą. Nuasmeninimas gali būti tinkama naudos išsaugojimo ir rizikos mažinimo strategija. Visiškai nuasmeninus duomenų rinkinį ir panaikinus galimybę nustatyti asmens tapatybę, tokiems duomenims nebetaikomi Europos Sąjungos duomenų apsaugos teisės aktai. Antra vertus, iš konkrečių atvejų tyrimų ir mokslinių straipsnių aiškiai matyti, kad, remiantis gausiu asmens duomenų rinkiniu, parengti visiškai anoniminį duomenų rinkinį ir kartu išsaugoti tiek jame esančios informacijos, kiek reikia užduočiai atlikti, nėra paprasta. Pavyzdžiui, anoniminiu laikomą duomenų rinkinį sujungus su kitu duomenų rinkiniu, gali atsirasti galimybė nustatyti vieno arba daugiau asmenų tapatybę“[79]. Taigi, Europos Komisijos teigimu viena iš priežasčių kuo asmens duomenų anonimizavimas gali būti naudingas duomenų valdytojui, yra naudos išsaugojimo ir rizikos mažinimo strategija, kitaip tariant anonimizavimas padeda duomenų valdytojui pasiekti jo norimų tikslų, nesukūriant dėl to rizikos nei duomenų subjektui, nei duomenų valdytojui. Tokios pozicijos taip pat laikosi ir Valstybinė duomenų apsaugos institucija nurodydama, kad „duomenų valdytojams nuasmeninimas gali būti vertingas kaip strategija, ypač atvirųjų duomenų panaudojimo reikmėms, kartu mažinant susijusiems asmenims gresiančius pavojus“[80].

Galima išskirti ir daugiau priežasčių kodėl asmens duomenų anonimizavimas gali būti naudinga duomenų saugumo priemonė. Autorius Balaji Raghunathan pabrėžia, kad tai gali būti poreikis apsaugoti jautrius duomenis, kurie yra tvarkomi siekiant naudoti juos verslo vystymo tikslais, taip pat priežastis gali būti dėl to, kad atsiranda daugiau netinkamo asmens duomenų tvarkymo pavyzdžių, ko pasekoje ir asmens duomenų apsaugos pažeidimų; didelė rizika įmonėms, ypač piniginių atžvilgiu dėl to, kad jie galbūt netinkamai tvarko asmens duomenis, taip pat rizika perduodant tokius duomenis, net ir teisėtai[81]. Minėtas autorius taip pat pažymi, jog vis daugėja atvejų, kai draudimo bendrovės sutinka apdrausti juridinius asmenius tik tuo atveju, jeigu pas juos yra įdiegta tinkama asmens duomenų apsaugos sistema; be to jis pažymi, kad asmens duomenų anonimizavimas taip pat gali lemti mažesnes draudimo įmokos išlaidas, pavyzdžiui kai įmonė draudžiasi nuo asmens

---

[78] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 3 psl.
[79] *Ibid*, 5 psl.
[80] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf, 1 psl.
[81] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf, 5 psl.

duomenų praradimo rizikos[82]. Balaji Raghunathan rašė, jog remdamasis tyrimais iš įvairių elektroninių nusikaltimų forumų, vienas iš pirmaujančių JAV laikraščių rado įdomią statistiką apie juodąją privačių duomenų rinką. Tyrimas rodo, kad nutekėjus informacijai apie vairuotojo pažymėjimą vienam asmeniui galima sukelti nuo 100 iki 200 dolerių nuostolių, o atsiskaitymo duomenys, gimimo data ir kredito kortelės numeris gali sukelti dar didesnę žalą[83]. Taip pat šis autorius nurodo, kad piniginė nauda nėra vienintelė priežastis, kodėl verta apsaugoti asmens duomenis; pasitaikė atvejų, kai buvę įmonės darbuotojai, siekdami būti sugrąžinti į ankstesnį darbą nutenkindavo ar kitaip netinkamai panaudodavo įmonės klientų asmens duomenis, ko pasekoje įmonei tai sukėlė prastą įvaizdį ir kitas neigiamas pasekmes[84]. Šis autorius taip pat pabrėžia, kad nepaisant to, kad yra teisės aktais sureguliuota asmens duomenų apsauga, tam tikros įmonės vis tiek piktnaudžiauja ir savo klientų duomenis, kurie buvo surinkti išskirtinai paslaugų teikimo tikslais, yra naudojami rinkodaros ar kitais tikslais ir šių duomenų savininkai apie tai net nežino[85]. Taigi, autorius daro išvadą, kad asmens duomenų anonimizavimas iš esmės gali būti naudingas tiek duomenų subjektui, tiek duomenų valdytojui. Duomenų subjektui asmens duomenų anonimizavimas gali užtikrinti, kad jo duomenys bus apsaugoti bei jo tapatybė nebus nustatyta. O duomenų valdytojui asmens duomenų anonimizavimas gali daryti teigiamą įtaką verslo santykiuose ir padėti atitikti asmens duomenų apsaugos reikalavimų.

Bendrasis duomenų apsaugos reglamentas 89 straipsnyje nurodo, kad tvarkant duomenis archyvavimo tikslais, viešojo intereso labui, mokslinių ar istorinių tyrimų tikslais arba statistiniais tikslais, tokiam tvarkymui turi būti taikomos tokios techninės ir organizacinės priemonės, kurios užtikrintų duomenų kiekio mažinimo principą. Duomenų kiekio mažinimo principas iš esmės reiškia, kad turi būti užtikrinamas tinkamas duomenų tvarkymo tikslų ir duomenų apimties santykis[86]. Taip pat remiantis BDAR duomenų kiekio mažinimo principas nurodo, jog turi būti renkami adekvatūs, tinkami ir tik tokie, kurių reikia siekiant tikslų, dėl kurių jie tvarkomi asmens duomenys. Julius Zaleskis savo monografijoje atskleidžia aptariamo principo ir asmens duomenų anonimizavimo santykį: „duomenų kiekio mažinimo principo taikymas ir iš jo kylantis būtinumo reikalavimas skatina duomenis nuasmeninti“[87]. Atsižvelgiant į tai, autorius linkęs manyti, kad asmens duomenų anonimizavimas yra susijęs su duomenų kiekio mažinimo įgyvendinimo principu, kadangi tuo atveju, kai duomenų valdytojas gali pasiekti savo tikslų, pavyzdžiui statistinių, naudojant tik anoniminius

---

[82] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf,12 psl.
[83] *Ibid*, 6 psl.
[84] *Ibid*, 6 psl.
[85] *Ibid*, 7 psl.
[86] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019),121 psl.
[87] *Ibid*, 123 psl.

duomenis, jis ir turėtų asmens duomenis anonimizuoti, nes kitaip gautųsi, kad duomenų valdytojas tvarko perteklinius, tikslui pasiekti nereikalingus asmens duomenis, o tą daryti draudžia BDAR.

Taigi, asmens duomenų anonimizavimo paskirtis yra trejopa. Pirmiausia, anonimizavimas tai naudos išsaugojimo ir rizikos mažinimo strategija, kuri užtikrina duomenų valdytojui galimybę tvarkyti duomenis atitinkamais tikslais, nesukeliant duomenų apsaugos pažeidimo rizikos. Antra, anonimizavimas užtikrina tinkamą duomenų apsaugą duomenų subjektams. Ir trečia, anonimizavimas padeda įgyvendinti BDAR įtvirtintą duomenų kiekio mažinimo principą. Be to, pastebėtina, kad šiuo procesu taip pat gali būti užtikrinama pusiausvyra, kuri pasireiškia duomenų valdytojo noru pasiekti savo iškeltų tikslų bei duomenų subjekto lūkesčiu, kad jo duomenys būtų tinkamai apsaugoti.

1.3.2. Pagrindiniai anonimizavimui taikomi reikalavimai

Grįžtant prie asmens duomenų anonomizavimo apibrėžimo, pažymėtina, kad anonimizavimas taip pat apibrėžiamas ir tarptautiniuose standartuose, pvz., ISO 29100[88]. Šis standartas nurodo, kad „asmens duomenų anonimizavimas yra procedūra, pagal kurią asmens tapatybės informacija nesugrąžinamai pakeičiama taip, kad asmens tapatybės informacijos valdytojas pats vienas arba bendradarbiaudamas su kita šalimi nebegalėtų tiesiogiai arba netiesiogiai nustatyti asmens tapatybės informacijos savininko tapatybės“[89]. „Atlikto asmens duomenų pakeitimo, susijusio su galimybe tiesiogiai arba netiesiogiai nustatyti asmens tapatybę, negrąžinamumas taip pat labai svarbus ISO aspektas. [...] Tai pasakytina ir apie apibrėžtis, pateiktas kai kurių šalių (pvz., Italijos, Vokietijos ir Slovėnijos) teisės aktuose, kuriuose daugiausia dėmesio skiriama galimybės nustatyti asmens tapatybę nebuvimui ir vartojama neproporcingų pastangų, kuriomis siekiama pakartotinai nustatyti asmens tapatybę, sąvoka. Tačiau Prancūzijos duomenų apsaugos įstatyme nustatyta, kad duomenys išlieka asmens duomenimis net ir tuo atveju, kai labai sunku ar beveik neįmanoma pakartotinai nustatyti duomenų subjektą, t. y. šiame įstatyme nėra nuostatos, kurioje būtų minimas „galimumo“ kriterijus“[90]. Šiuo atveju, autorius nori atkreipti dėmesį, kad yra pabrėžiamas skirtingas kai kurių Europos šalių požiūris į vieną svarbiausių asmens duomenų anonimizavimui taikomą reikalavimą – negalėjimą identifikuoti asmenį. Remiantis išdėstyta informaciją, galima daryti prielaidą, jog egzistuoja du požiūriai: 1) asmens tapatybė negali būti nustatyta atsižvelgiant į

---

[88] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 6 psl.
[89] *Ibid*, 6 psl.
[90] *Ibid*, 6 psl.

proporcingas pastangas ją nustatyti ir 2) griežtas negalėjimas nustatyti asmens tapatybės net ir įdėjus neproporcingai dideles pastangas. Lietuvos požiūrį šiuo klausimu šiai dienai sunku tiksliai nustatyti, tačiau pažvelgus į Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 2013-01-01 – 2018-07-15 suvestinės redakciją, galima daryti išvadą, kad Lietuva laikėsi pirmojo požiūrio, t.y., kad asmens tapatybė negali būti nustatyta atsižvelgiant į proporcingas pastangas ją nustatyti[91]. Šioje suvestinėje buvo pateikiamas asmens duomenų anoniminimo apibrėžimas ir buvo nurodoma, kad anoniminimas yra „asmens duomenų pakeitimas taip, kad jie nebegalėtų būti siejami su fiziniu asmeniu, kurio tapatybė yra žinoma arba gali būti tiesiogiai ar netiesiogiai nustatyta, arba galėtų būti su juo siejami tik įdėjus pernelyg daug laiko, lėšų ir darbo“, kitaip tariant įdėjus neproporcingas pastangas tapatybei nustatyti. Autorius taip pat turi pagrindą manyti, kad dabartinis Europos Sąjungos reguliavimas šiuo klausimu taip pat yra linkęs palaikyti pirmąjį požiūrį, kuris sako, jog reikėtų atsižvelgti į proporcingas pastangas asmens tapatybei nustatyti. Tokia išvada seka iš BDAR preambulės 26 straipsnio, kuris be kita ko nurodo, jog nustatant asmens tapatybę reikėtų atsižvelgti į objektyvius veiksnius, tokius kaip sąnaudos, laikas ir kita.

Dar vienas svarbus aspektas yra asmens duomenų anonimizavimo teisėtumas arba kitaip tariant šio proceso teisėtumo reikalavimas. Kaip jau buvo minėta, Europos Komisija pažymi, kad anonimizavimas yra tolesnio tvarkymo atvejis, kuris turi atitikti suderinamumo reikalavimą, t.y. iš pat pradžių buvo renkami asmens duomenys, kurie turėjo atitikti asmens duomenų apsaugos reikalavimus[92]. Pasak Europos Komisijos darbo grupės, asmens duomenų anonimizavimo teisiniu pagrindu gali būti bet kuris, iš jau dabar BDAR nurodytų duomenų tvarkymo pagrindų[93]. BDAR 6 straipsnis numato šiuos teisinius duomenų tvarkymo pagrindus: sutikimas, sutartis, gyvybiniai duomenų subjekto ar kito fizinio asmens interesai, užduotis, vykdomą viešojo intereso labui arba vykdant duomenų valdytojui pavestas viešosios valdžios funkcijas ir teisėtas duomenų valdytojo ar trečiojo asmens interesas. Europos Komisijos darbo grupė mano, kad asmens duomenų anonimizavimas gali būti suderintas su pirminiais tikslais tik tuo atveju, jeigu anoniminė informacija bus parengta pagal visas anonimizavimo taisykles[94]. Tačiau, šioje vietoje autoriui kyla klausimas, ar tikrai asmens duomenų anonimizavimui yra reikalingas teisinis pagrindas, kuris yra būdingas asmens

---

[91] „Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas“, *Valstybės žinios*, (2011).

[92] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 7 psl.

[93] *Ibid*, 7 psl.

[94] Europos Komisija, *op.cit.*, 8 psl.

duomenims? Autoriaus abejonės yra paremtos tuo, kad BDAR preambulė nurodo, jog anoniminiai informacijai nėra taikomi asmens duomenų apsaugai keliami reikalavimai, todėl autoriaus manymu, jiems neturėtų būti taikomas ir reikalavimas dėl duomenų tvarkymo pagrindo bei tikslo. Informacijos komisaro biuro (ICO) nuomone, toks teisinis pagrindas kaip sutikimas, paprastai nėra reikalingas asmens duomenų anonimizavimui[95]. ICO pabrėžia, kad sutikimo turėjimas bet kuriuo atveju yra saugesnis pasirinkimas, tačiau jų manymu tai nėra būtina. Jie teigia, kad jeigu nėra tikimybės, jog asmens duomenų anonimizavimas sukels nepagrįstą žalą duomenų subjektui, tokiu atveju nėra prievolės turėti sutikimą, kad asmens duomenų anonimizavimas būtų laikomas teisėtu[96]. Be to, yra pabrėžiama tokio teisinio pagrindo grėsmė, kadangi sutikimas pagal savo esmę gali būti bet kada atšauktas, toks duomenų subjekto veiksmas gali sukelti rūpesčių ir tokia užduotis gali būti sunkiai įveikiama, ypač tuo atveju, kai būtų siekiama panaikinti viešai paskelbtą anoniminę informaciją[97]. Autorius yra linkęs palaikyti antrąjį požiūrį, kadangi taip pat mato grėsmę dėl teisinio pagrindo pasibaigimo ir negalėjimo sugrąžinti anoniminius duomenis į pradinę padėtį.

Taigi, apibendrinant asmens duomenų anonimizavimui taikomus reikalavimus, daroma išvadą, kad ko gero būtų sunku vienareikšmiškai nustatyti kokie tikslūs reikalavimai keliami asmens duomenų anonimizavimui. Toks kontraversiškas požiūris kyla iš to, jog kaip buvo išsiaiškinta, kai kurios valstybės gali skirtingai interpretuoti negalėjimą nustatyti asmens tapatybę, vieni laikosi griežto požiūrio dėl negalėjimo asmens identifikuoti, kiti šiek tiek nuolankesnio, kuris teigia, jog reikia atsižvelgti į proporcingas pastangas tapatybę nustatyti. Taip pat pasakytina ir apie kitą teisėtumo reikalavimą, kadangi buvo nustatyta, jog ko gero nėra bendros nuomonės ar asmens duomenų anonimizavimui yra reikalingas vienas iš BDAR įtvirtintų teisėtumo pagrindų, ar ne.

---

[95] Personal Data protection commission Singapore, *„Guide to basic data anonymisation techniques“*, (IAPP, 2018). Prieiga per internetą: https://iapp.org/media/pdf/resource_center/Guide_to_Anonymisation.pdf, 28 psl.
[96] *Ibid*, 28 psl.
[97] *Ibid*, 29 psl.

2. ANONIMIZAVIMAS IR KITOS DUOMENŲ SAUGUMO PRIEMONĖS

2.1. Tinkamų duomenų saugumo priemonių samprata

BDAR įtvirtintas duomenų saugumo principas reikalauja, kad būtų užtikrintos tinkamos techninės ir organizacinės duomenų saugumo priemonės[98]. Šios priemonės turi apsaugoti asmens duomenis nuo netyčinio ar neteisėto naudojimo, pakeitimo, atskleidimo, platinimo, sunaikinimo ir pan.[99]. Nagrinėjant asmens duomenų anonimizavimo sampratą, autorius susidūrė su mintimi, jog asmens duomenų anonimizavimas kartais tapatinamas su kitomis duomenų saugumo priemonėmis, pavyzdžiui pseudomininizavimu, šifravimu[100], teismo sprendimų ar kitų dokumentų nuasmeninimu[101]. Siekiant paneigti šią nuomonę bei išvengti tokių klaidingų tapatinimų, šiame skyriuje bus atribojamos kitos duomenų saugumo priemonės nuo asmens duomenų anonimizavimo, nustatomi panašumai ir trūkumai šių priemonių. Tačiau pirmiausia siekiama išsiaiškinti kokia yra tinkamų duomenų saugumo priemonių samprata.

Julius Zaleskis rašė, kad „galima skirti kelias duomenų saugumo priemonių rūšis“[102]. „Pagal duomenų saugumo priemonių pobūdį, galima skirti technines ir organizacines duomenų saugumo priemones. Pagal teisinį sureguliavimą, galima skirti tas duomenų saugumo priemones, kurios yra nustatytos, ir tas, kuriuos nėra nustatytos. [...] Techninių duomenų saugumo priemonių sąvoka apima mechanizmus, įrangą ir įrankius, skirtus užtikrinti informacijos saugumą. [...] Organizacinės duomenų saugumo priemonės yra susijusios su tuo, kaip organizacija yra įsteigta ir vykdo veiklą. [...] BDAR nustatytos kelios konkrečios duomenų saugumo priemonės. Daugelių atvejų šios priemonės yra tinkamos užtikrinti tinkamą saugumą ir turėtų būti įgyvendintos“[103]. Šioje vietoje autorius nori pabrėžti, kad šio mokslinio darbo tyrimo prasme yra aktualūs tik techninės duomenų saugumo priemonės, nes būtent su jomis gali būti tapatinamas asmens duomenų anonimizavimas. Techninės duomenų saugumo priemonės gali būti: asmens duomenų pseudominizavimas, šifravimas,

---

[98] European Union Agency for Fundamental Rights and Council of Europe, *„Handbook on European data protection law*“, (Luxembourg: Council of Europe, 2018), 131 psl.
[99] Aurelia Tamò-Larrieux, *„Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things“*, (Springer, 2018), 92 psl.
[100] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 11 psl.
[101] Lea Kisner, *„Deidentification versus anonymization“*, (IAPP, 2019). Prieiga prie interneto: https://iapp.org/news/a/de-identification-vs-anonymization/
[102] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 132 psl.
[103] *Ibid*, 132 psl.

reguliarus priemonių veiksmingumo vertinimas ir tikrinimas ir kita[104]. Organizacinių duomenų saugumo priemonių šio darbo kontekste neaktualu lyginti su asmens duomenų anonimizavimu.

BDAR 32 straipsnio 1 dalis numato, kad „atsižvelgdamas į techninių galimybių išsivystymo lygį, įgyvendinimo sąnaudas bei duomenų tvarkymo pobūdį, aprėptį, kontekstą ir tikslus, taip pat duomenų tvarkymo keliamus įvairios tikimybės ir rimtumo pavojus fizinių asmenų teisėms ir laisvėms, duomenų valdytojas ir duomenų tvarkytojas įgyvendina tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas, įskaitant, inter alia, jei reikia: a) pseudonimų suteikimą asmens duomenims ir jų šifravimą; b) gebėjimą užtikrinti nuolatinį duomenų tvarkymo sistemų ir paslaugų konfidencialumą, vientisumą, prieinamumą ir atsparumą; c) gebėjimą laiku atkurti sąlygas ir galimybes naudotis asmens duomenimis fizinio ar techninio incidento atveju; d) reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą“. Šiame straipsnyje Bendrasis duomenų apsaugos reglamentas pateikia tinkamų techninių ir organizacinių priemonių pavyzdinį sąrašą. Pažymėtina, kad asmens duomenų anonimizavimas į minėtą sąrašą nėra įtrauktas, bet yra paminėtos kitos duomenų apsaugos priemonės, tokios kaip pseudominizavimas, šifravimas ir kt. Tačiau šioje vietoje Julius Zaleskis rekomenduoja neapsiriboti vien BDAR tiesiogiai įtvirtintomis duomenų saugumo priemonėmis ir tvirtina, kad turi būti įgyvendintos visos tinkamos technines ir organizacines priemones, kurios užtikrintų tinkamą duomenų saugumą[105]. Taigi, autorius daro išvadą, kad pagrindinis kriterijus, kuris leidžia nustatyti ar duomenų saugumo priemonė yra tinkama arba ne, yra informacijos saugumas. Atsižvelgiant į tai autorius mano, kad nepaisant to, jog anonimizavimas nėra tiesiogiai įvardytas Reglamente kaip tinkama duomenų apsaugos priemonė, tokia situacija dar neduoda pagrindo manyti, jog asmens duomenų anonimizavimas nėra tinkama duomenų saugumo priemonė.

Nuomonę, kad asmens duomenų anonimizavimas galbūt nėra tinkama duomenų saugumo priemonė, galima paneigti Mindaugo Civilkos ir kitų „Informacinių technologijų teisė“ knygos autorių teiginiais, kurie nurodo, kad atsižvelgiant į technologijas ir jų įdiegimo išlaidas, tinkamos techninės ir organizacinės priemonės turi užtikrinti tokį saugumo lygį, kuris atitinka duomenų tvarkymo keliamą riziką ir saugotinų duomenų pobūdį[106]. Taip pat šie autoriai pažymi, kad „jautrūs duomenys interneto erdvėje turi būti anonimizuojami. Tai gali būti atlikta tiek įrenginių pagalba (pvz. užkodavimo algoritmas, įrašytas į intelektualiąsias korteles, tiek ir įdiegiant atitinkamą

[104] European Union Agency for Fundamental Rights and Council of Europe, *„Handbook on European data protection law*“, (Luxembourg: Council of Europe, 2018), 131 psl.
[105] Julius Zaleskis, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. (Vilnius: Registrų centras, 2019), 133 psl.
[106] Mindaugas Civilka ir kt., *„Informacinių technologijų teisė“*, (Vilnius, 2004), 129 psl.

funkciją (pvz. tvarkymas prižiūrimas patikimos trečiosios šalies, kuri saugo tikrąją asmens subjekto tapatybę)“[107]. Autoriaus manymu, minėti autoriai priskiria asmens duomenų anonimizavimą prie tinkamų duomenų saugumo priemonių. Panašios nuomonės laikosi ir Balaji Raghunathan, kuris pažymi, kad iš duomenų apsaugos teisės perspektyvos, asmens duomenų anonimizavimas yra tik viena populiariausių priemonių užtikrinti duomenų apsaugą; specifiniams duomenų apsaugos reikalavimams užtikrinti taip pat gali būti naudojami ir kiti metodai[108]. Atsižvelgiant į tai autorius taip pat linkęs palaikyti nuomonę, jog asmens duomenų anonimizavimas turi būti laikomas tinkama duomenų saugumo priemonė, nes kaip jau buvo išsiaiškinta anksčiau, anonimizavimas gali užtikrinti informacijos saugumą paversdamas duomenis anoniminiais ir tokiu būdu panaikina galimybę nustatyti duomenų subjektą.

Kalbant apie asmens duomenų saugumo priemonių pasirinkimą, rekomenduojama kiekvieną kartą atsižvelgti į konkrečią situaciją, įvertinti kokia rizika yra keliama asmens duomenims ir atsižvelgiant į tai rinktis tam tikrą techninę duomenų saugumo priemonę[109]. Renkantis atitinkamas duomenų saugumo priemones, taip pat rekomenduojama atsižvelgti į tokius veiksnius kaip techninės galimybės, rizika, kaštai, kokių priemonių būtų pakankama tinkamai duomenų apsaugai, kokios galbūt priemonės tinkamos duomenų apsaugos neužtikrina ir pan[110]. Techninės duomenų saugumo priemonės turi ne tik užtikrinti tinkamą duomenų apsaugą, bet jos turi būti ir parengtos taip, kad būtų išvengta perteklinio duomenų tvarkymo[111].

Apibendrinant, duomenų saugumo priemonė gali būti 2 rūšių, t.y. techninės duomenų saugumo priemonės ir organizacinės duomenų saugumo priemonės. Techninės priemonės užtikrina, kad atitinkama įranga, įrankiai ir kiti mechanizmai būtų tinkami siekiant apsaugoti asmens duomenis, o organizacinės duomenų saugumo priemonės yra susijusios su konkrečios bendrovės veiklos organizavimu asmens duomenų apsaugos atžvilgiu. Bendrasis duomenų apsaugos reglamentas numato tinkamų duomenų saugumo priemonių pavyzdinį sąrašą, kuriame atsispindi tokios techninės duomenų saugumo priemonės kaip pseudominizavimas, šifravimas ir kt., tačiau asmens duomenų anonimizavimas tiesiogiai jame nėra įtvirtintas. Atsižvelgiant į tai manoma, kad tai gali būti viena iš priežasčių kodėl asmens duomenų anonimizavimas yra tapatinamas su kitomis duomenų

---

[107] Mindaugas Civilka ir kt., *„Informacinių technologijų teisė“*, (Vilnius, 2004), 129 psl.
[108] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf, 10 psl.
[109] European Union Agency for Fundamental Rights and Council of Europe, *„Handbook on European data protection law*“, (Luxembourg: Council of Europe, 2018), 131 psl.
[110] Enrico Nardelli, Sabina Posadziejewski, Maurizio Talamo, *„Certification and Security in E-Services– From E-Government to E-Business”*, (Springer, 2013), 229 psl.
[111] *Ibid*, 229 psl.

priemonėmis. Būtent todėl yra svarbu ne tik atskleisti asmens duomenų anonimizavimo sąvoką, bet ir aiškiai atriboti ją nuo kitų duomenų saugumo priemonių.

2.2. Pseudominizavimas, šifravimas ir jų atribojimas nuo asmens duomenų anonimizavimo

Kaip minėta, asmens duomenų anonimizavimas kartais gali būti tapatinamas su tokiomis duomenų saugumo priemonėmis kaip pseudominizavimas ir šifravimas. Todėl siekiant aiškiai atriboti asmens duomenų anonimizavimą nuo pseudominizavimo bei duomenų šifravimo, šiame skyriuje bus atskleidžiamos aptariamų duomenų saugumo priemonių sampratos ir jų skirtumai nuo asmens duomenų anonimizavimo.

Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 18 staipsnyje įstatymų leidėjas nurodo pseudonimų suteikimą, kaip tinkamą duomenų saugumo priemonę. Šis įstatymas taip pat pateikia ir pseudominizavimo apibrėžimą: „pseudonimų suteikimas – asmens duomenų tvarkymas taip, kad asmens duomenys nebegalėtų būti priskiriami konkrečiam duomenų subjektui nesinaudojant papildoma informacija, jeigu tokia papildoma informacija yra saugoma atskirai ir jai taikomos techninės bei organizacinės priemonės siekiant užtikrinti asmens duomenų nepriskyrimą fiziniam asmeniui, kurio tapatybė yra nustatyta arba kurio tapatybę galima nustatyti“. Remiantis minėto įstatymo apibrėžimu, galima daryti išvadą, kad pseudominizavimo proceso rezultatas yra duomenys, kurie nebegali būti priskiriami konkrečiam duomenų subjektui tik nepasinaudojant papildoma informacija. Atsižvelgiant į tai, autorius turi pagrindą manyti, kad asmens duomenų pseudominizavimo metu identifikatoriai nėra negrįžtamai pašalinami kaip asmens duomenų anonimizavimo atveju, o tiesiog yra nuslepiami atitinkamame duomenų rinkinyje.

BDAR preambulėje taip pat yra numatyta, kad „pseudonimų suteikimas asmens duomenims gali sumažinti atitinkamiems duomenų subjektams kylančius pavojus ir padėti duomenų valdytojams ir duomenų tvarkytojams įvykdyti savo duomenų apsaugos prievoles“. Toks teiginys vėl pabrėžia, kad pseudominizavimas nepanaikina asmens tapatybės nustatymo rizikos, o tik ją sumažina. Tuo tarpu asmens duomenų anonimizavimas, kaip jau buvo išsiaiškinta anksčiau, užtikrina, kad asmens duomenų tapatybė nebegalės būti nustatyta. Europos Komisija taip pat pažymi, kad pseudominizavimas anonimiškumo neužtikrina[112]. „Pseudonimų suteikimas – tai metodas, pagal kurį

[112] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 21 psl.

vienas požymis (paprastai – unikalus) įraše pakeičiamas kitu. Todėl išlieka galimybė netiesiogiai nustatyti fizinio asmens tapatybę; taigi vien pseudonimų suteikimas neužtikrina duomenų rinkinio anonimiškumo. [...] Taikant pseudonimų suteikimo metodą, sumažinama galimybė duomenų rinkinį susieti su pirmine duomenų subjekto tapatybe; taigi šis metodas yra naudinga saugumo priemonė, bet tai nėra anonimizavimo metodas. Pseudonimų suteikimo rezultatas gali nepriklausyti nuo pirminės vertės (pvz., jeigu tai atsitiktinis duomenų valdytojo sugeneruotas skaičius arba duomenų subjekto pasirinkta pavardė) arba gali būti sukuriamas naudojantis požymio arba jų grupės pirminėmis vertėmis, pvz., taikant maišos funkciją arba šifravimo sistemą“[113]. Taigi, Europos Komisija taip pat laikosi nuomonės, kad tiek pseudominizavimas, tiek anonimizavimas yra naudingos duomenų saugumo priemonės, tačiau jos yra skirtingos; iš esmės jos skiriasi tuo, kad anonimizavimas užtikrina duomenų rinkinio anonimiškumą, o pseudominizavimas tik sumažina tapatybės nustatymo riziką.

Siekiant plačiau atskleisti pseudominizavimo proceso veikimo mechanizmą, toliau yra pateikiamas pseudonimų suteikimo metodo pavyzdys: originalus sakinys – Čarli Spenser, gimęs 1967 m. balandžio 3 d., yra keturių vaikų tėvas, iš kurių yra du berniukai ir dvi mergaitės, o pseudominizuotas sakinys atrodytų taip – **Č. S. 1967** yra keturių vaikų tėvas, iš kurių yra du berniukai ir dvi mergaitės[114]. Kaip matoma iš šio pavyzdžio, asmens vardas bei pavardė buvo pakeisti tam tikrais pseudonimais – Č. S., šiuo konkrečiu atveju inicialais. Pastebėtina, kad tuo atveju, kai tokia informacija būtų naudojama pakankamai siaurame rate, pavyzdžiui mažame kaimelyje, ponas Čarli galėtų būti nesunkiai identifikuojamas[115]. Atsižvelgiant į tai manoma, kad pseudominizavimas ne visais atvejais gali būti veiksminga duomenų saugumo priemonė[116]. Šioje vietoje autorius nori atkreipti dėmesį, kad kaip jau buvo išsiaiškinta anksčiau, tinkamai atliktas anonimizavimas asmens identifikavimo rizikos neturėtų sukelti net ir siaurame rate.

Dar vienas labai svarbus aspektas yra tai, kad pagal Reglamentą „asmens duomenys, kuriems suteikti pseudonimai ir kurie galėtų būti priskirti fiziniam asmeniui pasinaudojus papildoma informacija, turėtų būti laikomi informacija apie fizinį asmenį, kurio tapatybė gali būti nustatyta“. Kitaip tariant turi būti laikomi asmens duomenimis. Pseudominizuoti duomenys yra anonimiški tik tam tikriems asmenims, pavyzdžiui tyrėjams, kurie tuos duomenis gauna ir naudoja atitinkamiems tikslams, tačiau duomenų valdytojas ar kita patikima šalis turi savo žinioje šių duomenų identifikatorius, vadinasi jiems šie duomenys nėra anoniminiai[117]. Atsižvelgiant į tai, Europos

---

[113] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 21 psl.
[114] European Union Agency for Fundamental Rights and Council of Europe, *„Handbook on European data protection law“*, (Luxembourg: Council of Europe, 2018), 131 psl.
[115] *Ibid*, 132 psl.
[116] *Ibid*, 132 psl.
[117] *Ibid*, 132 psl.

Sąjungoje pseudominizuoti duomenys yra laikomi asmens duomenimis, tuo tarpu anonimizuoti duomenys nėra laikomi[118]. Tokios nuomonės laikosi ir Alan Calder, kuris teigia, kad nepaisant to, kad Bendrajame duomenų apsaugos reglamente pseudominizavimas vertinamas teigiamai ir kaip tinkama duomenų saugumo priemonė, vis dėl to nurodoma, kad duomenys, kuriems buvo suteikti pseudonimai, turėtų būti laikomi, kaip asmenį identifikuojantis duomenys, nes panaudojus papildomą informaciją, tapatybę galima nustatyti[119]. Atsižvelgiant į tai, organizacijos pasirinkusios taikyti pseudominizavimą, kaip priemonę apsaugoti asmens duomenis, turi užtikrinti, kad asmens duomenys bus apsaugoti nuo duomenų subjekto identifikavimo, net ir panaudojus papildomą informaciją[120]. Pažymėtina, kad kaip jau buvo išsiaiškinta 1.2. skyriuje, anoniminiai duomenys nėra laikomi asmens duomenimis ir jiems nėra taikomi asmens duomenų apsaugą reglamentuojantys teisės aktai bei principai. Atsižvelgiant į tai autorius daro išvadą, kad tai yra dar vienas pseudominizavimo skirtumas nuo asmens duomenų anonimizavimo.

Reglamento preambulėje taip pat nurodoma, kad „siekiant užtikrinti saugumą ir užkirsti kelią šį reglamentą pažeidžiančiam duomenų tvarkymui, duomenų valdytojas arba duomenų tvarkytojas turėtų įvertinti su duomenų tvarkymu susijusius pavojus ir įgyvendinti jo mažinimo priemones, pavyzdžiui, šifravimą“. Šifravimas yra kita aptariama duomenų saugumo priemonė. Techniškai duomenų šifravimas reiškia techniką, kuri pakeičia duomenis specialiaisiais ženklais[121]. Tradiciškai šifruojant asmens duomenis, jų identifikatoriai nėra panaikinami ir tokius duomenis galima sugrąžinti į pradinę padėtį pasinaudojant atitinkamu šifru arba taip vadinamuoju raktu. Kaip analogiją yra pateikiamas pavyzdys, kad lyg duomenys būtų uždaryti į tam tikrą dežę[122]. Teoriškai, šifruoti duomenys nėra iš tikrųjų anoniminiai duomenys, kadangi anoniminiai duomenys negali būti atkūriami, jie panaikina tapatybės nustatymo galimybę negrįžtamai[123]. Taigi ir šiuo atveju yra pabrėžiama, kad šifravimas laikomas tinkama duomenų saugumo priemonė, tačiau panašiai kaip ir pseudominizavimas, ši priemonė negali garantuoti, jog asmens tapatybė negalės būti nustatyta, kadangi ji nėra negrįžtamai pašalinama, kaip tai būtų asmens duomenų anonimizavimo atveju.

Europos Komisija pabrėžia, kad „labai klaidinga manyti, kad anonimizavimas yra tas pats, kas šifravimas arba kodavimas naudojant raktą. Ši klaidinga nuomonė grindžiama dviem prielaidomis: a) kadangi šifravimas taikomas kai kuriems duomenų bazės įrašo požymiams (pvz.,

---

[118] John C. Lindon, Jeremy K. Nicholson, Elaine Holmes, *„The Handbook of Metabolic Phenotyping“*, (Elsevier, 2018), 356 psl.
[119] Alan Calder, *„EU GDPR & EU-US Privacy Shield– A Pocket Guide“*, (United Kingdom, 2016), 27-28 psl.
[120] *Ibid*, 27-28 psl.
[121] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf, 4 psl.
[122] Jack M. Balkin ir kt., *„Cybercrime Digital Cops in a Networked Environment“*. (New York University Press, 2007), 168 psl.
[123] *Ibid*,168 psl.

vardui, pavardei, adresui, gimimo datai) arba šie požymiai pakeičiami iš pažiūros randomizuota eilute, sudaroma taikant kodavimo naudojant raktą operaciją, pvz., rakto naudojimu pagrįstos maišos funkciją, tai įrašas yra nuasmenintas; b) nuasmeninimas bus veiksmingesnis, jeigu raktas bus tinkamo ilgio ir šifravimo algoritmas bus pažangus“[124]. „Pirmiausia šių metodų tikslai yra visiškai skirtingi: šifravimas, kaip saugumo priemonė, yra skirtas ryšių linijos tarp nustatytų šalių (žmonių, įtaisų ar programinės arba aparatinės įrangos dalių) slaptumui užtikrinti, siekiant išvengti slapto pasiklausymo arba nepageidaujamo informacijos atskleidimo. Rakto naudojimu pagrįstas kodavimas – tai reikšminis duomenų pakeitimas naudojant slaptą raktą. Kita vertus, anonimizavimo tikslas – panaikinti galimybę nustatyti asmens tapatybę, neleidžiant slapta susieti požymių su duomenų subjektu. Nei šifravimas, nei rakto naudojimu pagrįstas kodavimas nėra tinkami duomenų subjekto tapatybės nustatymo galimybei panaikinti: kadangi bent vienas asmuo, t.y. duomenų valdytojas, tebeturi pirminius duomenis, išlieka galimybė gauti arba nustatyti pirminius duomenis. Atliekant tik reikšminį asmens duomenų pakeitimą, kaip tai daroma taikant rakto naudojimu pagrįstą kodavimą, nepanaikinama galimybė atkurti pirminę duomenų struktūrą pritaikius atvirkštinį algoritmą, surengus jėgos išpuolius (konkretus būdas priklauso nuo sistemų pobūdžio) arba nutekinus duomenis. Pažangiais šifravimo metodais galima užtikrinti, kad duomenys būtų geriau apsaugoti, t. y. taptų nesuprantami asmenims, nenaudojantiems iššifravimo rakto, tačiau duomenys nebūtinai tampa anonimizuoti. Kol yra pirminių duomenų raktas (net jeigu jį turi patikima trečioji šalis, pagal sutartį privalanti teikti saugią rakto deponavimo paslaugą), galimybė nustatyti duomenų subjekto tapatybę nepanaikinama“[125]. Taigi, galima daryti išvadą, jog duomenų šifravimas ir asmens duomenų anonimizavimas yra skirtingos duomenų saugumo priemonės. Galima išskirti 2 pagrindinius asmens duomenų anonimizavimo bei šifravimo skirtumus, t.y. 1) šifravimas nepanaikina galimybes nustatyti tapatybę, tuo tarpu anonimizavimas tokią galimybę suteikia ir 2) anonimizavimas – siekia negrįžtamai pašalinti identifikatorius, taip užtikrinant duomenų apsaugą, o šifravimas – užtikrina duomenų slaptumą, tačiau duomenų valdytojas ir (ar) kiti asmenys turi prieigą prie pirminių asmens duomenų.

Apibendrinant, galima daryti išvadą, kad tokios duomenų saugumo priemonės kaip asmens duomenų pseudominizavimas bei šifravimas skiriasi nuo asmens duomenų anonimizavimo ir jų nederėtų tapatinti. Šių duomenų saugumo priemonių tikslai iš esmės yra panašūs – užtikrinti duomenų apsaugą, jų slaptumą, išvengti duomenų saugumo pažeidimus. Tačiau vertinant šių priemonių mechanizmus bei rezultatus, jų turinys ženkliai skiriasi. Asmens duomenų anonimizavimas yra skirtas negrįžtamai panaikinti galimybę nustatyti asmens duomenis, tuo tarpu pseudominizavimas ir šifravimas tokios galimybes nepanaikina. Visų šių metodų pagalba galima

---

[124] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 31 psl.
[125] *Ibid*, 31 psl.

užtikrinti tinkamą duomenų apsaugą ir sumažinti duomenų saugumo pažeidimo riziką, tačiau pseudominizavimo ir šifravimo atveju asmens tapatybės nustatymo rizika negali būti visiškai panaikinta, kadangi pirminiai duomenys išlieka bent jau pas duomenų valdytoją, o tai reiškia, kad ir duomenų pažeidimo rizika, bent jau teoriškai egzistuoja. Taip pat šios duomenų saugumo priemonės skiriasi savo teisiniu reguliavimu, kadangi anonimizuotam duomenų rinkiniui nėra taikomi asmens duomenų apsaugos teisės aktai, tuo tarpu pseudominizuotiems ir užšifruotiems asmens duomenims vis dar lieka galioti BDAR ir kiti asmens duomenų apsaugą reglamentuojantys teisės aktai, nes jie ir po apdorojimo išlieka asmens duomenimis.

2.3. Teismo sprendimų nuasmeninimas ir asmens duomenų anonimizavimas

Autoriaus pastebėjimu, sąvokos asmens duomenų anonimizavimas ir nuasmenimimas tam tikrais atvejais gali būti sinonimais, o tam tikrais ne. Tai priklauso nuo to, ką tuo metu konkretus autorius, duomenų valdytojas, ar dar kitas asmuo turi omenyje. Šio darbo autorius turi pagrindą manyti, kad asmens duomenų anonimizavimas tam tikrais atvejais gali būti klaidingai tapatinimas su teismo procesinių sprendimų ar kitų dokumentų nuasmeninimu. Tokia išvada kyla atsižvelgiant į tai, kad nagrinėjant įvairius šaltinius dėl asmens duomenų anonimizavimo, iš anglų kalbos žodis *„anonymization“* į lietuvių kalbą verčiamas skirtingai. Pavyzdžiui, Europos Komisijos nuomonėje dėl nuasmeninimo metodų[126] ir Valstybinės duomenų apsaugos inspekcijos rekomendacijoje dėl nuasmeninimo metodų[127], anonimizavimas vadinamas nuasmeninimu. Taip pat žiūrint į Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymo 2013-01-01 – 2018-07-15 suvestinės redakciją, ten apibrėžiant anonimizavimą buvo vartojama sąvoka anoniminimas. Atsižvelgiant į tai autorius daro prielaidą, kad yra poreikis atskleisti nuasmeninimo sampratą bei atriboti ją nuo asmens duomenų anonimizavimo.

2015 m. Teismo Tarybos nutarime dėl teismų procesinių sprendimų bei teisėjų drausmės bylose priimtų sprendimų viešo skelbimo tvarkos patvirtinimo (toliau – Teismo Tarybos nutarimas) yra įtvirtintas teismo procesinių sprendimų nuasmeninimas. Šio nutarimo 11 punktas teigia, kad „jeigu teismų procesiniuose sprendimuose ir teisėjų drausmės bylose priimtuose sprendimuose minimi fizinių asmenų vardai ir pavardės, viešai skelbtinoje versijoje fizinių asmenų

---

[126] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 1 psl.

[127] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf, 1 psl.

vardai ir pavardės keičiami inicialais – pirmosiomis fizinių asmenų vardų ir pavardžių raidėmis. Ši nuostata netaikoma teisėjų (įskaitant teisėjus, kuriems buvo iškelta drausmės byla), teismo posėdžio sekretorių, vertėjų, ekspertų, specialistų, pareigūnų, prokurorų, antstolių, notarų, advokatų ar advokatų padėjėjų, bankrutuojančių įmonių administratorių ar jų padėjėjų, teismo mediatorių vardams ir pavardėms“[128]. „Lietuvos teismų sprendimų nuasmeninimo taisyklėse nurodytos keturios šių duomenų rūšys, kurios neturėtų būti skelbiamos teismo sprendimuose: (1) valstybės, valstybės tarnybos, profesinės ar komercinės veiklos, bankų ir kitos įstatymų saugomos paslaptys; 2) identifikavimo numeris, gyvenamųjų vietų adresai, gimimo datos ir vieta, santuokos, skyrybos ir mirtis; 3) duomenis, leidžiančius identifikuoti fiziniams asmenims priklausantį ar kitu teisėtu pagrindu valdomą turtą – valstybinių automobilių numeriai, banko sąskaitų numeriai, unikalūs nekilnojamojo turto numeriai, šio turto buvimo vieta, kiti turto rekvizitai; 4) kita bylos medžiaga, teismo nutartimi ar įstatymu pripažinta nevieša, išskyrus teismo sprendimų argumentus, turinčius reikšmės vienodam įstatymų aiškinimui ir taikymui, jei jie nepažeidžia visų pripažinimo tikslų medžiaga (ar jos dalis) kaip nevieša bylos nagrinėjimo eiga“[129]. Vertinant pateiktus apibrėžimus galima daryti išvadą, kad teismai taip pat siekia atitikti asmens duomenų apsaugos reikalavimus, užtikrinti bylos šalims ir kitiems asmenims tinkamą jų duomenų apsaugą, todėl nusistatė aiškias taisykles kokie asmens duomenys apskritai neturėtų būti skelbiami viešai ir kokie turi būti nuasmeninami.

Atsižvelgiant į Teismo Tarybos nutarimą, teismo procesinių sprendimų nuasmeninimas yra teismo proceso šalių vardų ir pavardžių pakeitimas inicialais, priklausančiais tam pačiam asmeniui. Pavyzdžiui 2019 m. lapkričio 29 d. byloje asmens duomenys nuasmeninti taip: „Ieškovė bankrutavusi uždaroji akcinė bendrovė (toliau – BUAB) „Edrija“ kreipėsi į teismą su ieškiniu atsakovams **E. D. ir I. D**., kuriuo prašė pripažinti 2016 m. gruodžio 29 d. akcijų pirkimo–pardavimo sutartį negaliojančia nuo sudarymo momento ir taikyti restituciją – solidariai priteisti iš atsakovų 276 808,39 Eur, 6 proc. delspinigius ir bylinėjimosi išlaidas“[130]. Taip pat kitoje baudžiamojoje byloje asmens duomenys buvo nuasmeninti tokiu būdu: „T. Š. nuteistas už tai, kad, dirbdamas UAB „DC (-)“, įmonės kodas (-), produktų specialistu, veikdamas tyčia, iš (-) socialinės globos namų, įmonės kodas (-), esančių adresu (-), (-) k., (-) r., vyriausiosios slaugytojos V. P. gavo jos žinioje esančius (-) socialinės globos namų gyventojų: P. P., A. Š., J. J., K. N., O. V., S. B., M. S., M. R., R. V., O.

[128] „Teisėjų Tarybos 2015 m. lapkričio 27 d. nutarimas dėl teismų procesinių sprendimų bei teisėjų drausmės bylose priimtų sprendimų viešo skelbimo tvarkos patvirtinimo Nr. 13P- 146-(7.1.2)“, TAR, (2015).
[129] Edita Gruodytė, Saulė Milčiuvienė, *„Anonymization of court decisions in the EU: actual and comparative issues“*, Teisės apžvalga Nr. 2 (18), (2018). Prieiga per internetą: https://www.vdu.lt/cris/bitstream/20.500.12259/60444/1/ISSN2029-4239_2018_N_2_18.PG_60-70.pdf, 64 psl.
[130] „Lietuvos apeliacinis teismo nutartis 2019 m. lapkričio 29 d. civilinėje byloje Nr. E2-1205-302/2019”, E-teismai: https://eteismai.lt/byla/118204413422338/e2-1205-302/2019?word=teism%C5%B3%20nutartys%20lat

B., R. P., L. M., J. Ž., S. A., V. K., E. V., V. Č., A. I., A. J., R. D., V. D., V. K., T. B., I. P., V. G., D. A., N. G., V. M., N. Č., R. B., B. J. B., S. A. J. kompensuojamųjų vaistų pasus, užpildė Lietuvos Respublikos sveikatos apsaugos ministerijos ar asmens sveikatos priežiūros įstaigos administracijos teisės aktų nepatvirtintus žaizdos įvertinimo protokolus“[131]. Iš šių pavyzdžių aiškiai matyti, kad tokie asmens duomenys kaip vardas ir pavardė nuasmeninami pakeičiant šiuos duomenis atitinkamais inicialais, o kiti duomenys yra tiesiog neskelbiami. Šio darbo autoriaus manymu, kalbant apie teismo procesinių sprendimų nuasmeninimą, reikia turėti omenyje, jog toks fizinių asmens duomenų pašalinimas yra aktualus tik rengiant ir į vieša erdvę talpinant atitinkamą teismo sprendimą. Algimantas Šideikis rašė, kad „pagal susiklosčiusią praktiką bylos šalių pavardės šiuo metu yra paskelbiamos teismo posėdžio dieną teismo skelbimų lentoje ir skelbiamos teismo posėdžio metu. Vėliau tokia informacija yra saugoma teismų archyvuose. Viešajai erdvei prieinamose teismų procesinių sprendimų elektroninėse duomenų bazėse, teismų (Lietuvos Aukščiausiojo Teismo, Lietuvos vyriausiojo administracinio teismo, kitų teismų) tinklalapiuose, Liteko duomenų bazėse, priėmus TT nutarimą, bylos šalių duomenys yra nuasmeninti“[132]. Atsižvelgiant į tai galima daryti išvadą, kad teismo sprendimų nuasmeninimas neužtikrina fizinio asmens anonimiškumo tokia apimtimi, kokia jį užtikrina asmens duomenų anonimizavimas ir tai jau yra vienas iš pagrindinių asmens duomenų anonimizavimo ir nuasmeninimo skirtumų. Autoriaus manymu, nuasmeninimas yra tik tam tikras asmens duomenų slėpimas iš viešosios erdvės, kaip pavyzdžiui pseudominizavimo ir šifravimo atveju, tik panaudojus kitokią techniką, tačiau originalūs duomenys nebūna visiškai ir negrįžtamai pašalinti.

Algimantas Šideikis teigia, kad yra nustatyta speciali susipažinimo su teismo bylos medžiaga ir bylos šalimis tvarka[133]. Tai reiškia, kad teismo procesinių sprendimų nuasmeninimas dar skiriasi nuo asmens duomenų anonimizavimo ir tuo, kad egzistuoja ne tik teorinė galimybė pagal nuasmenintus duomenis, t.y. pagal fizinio asmens inicialus, nustatyti konkretaus asmens tapatybę, tačiau tai dar galima padaryti ir tiesiogiai kreipiantis į teismą dėl nuasmenintos informacijos atskleidimo. Pavyzdžiui 2016 m. gruodžio 12 d. Lietuvos vyriausiasis administracinis teismas sprendė ginčą, kuriuo metu Klaipėdos daugiavaikių šeimų bendrija kreipėsi į teismą su skundu, prašydama panaikinti Klaipėdos miesto savivaldybės administracijos direktoriaus sprendimą „Dėl nuasmeninto Klaipėdos miesto savivaldybės tarybos sprendimo“ ir įpareigoti Klaipėdos miesto savivaldybės tarybą pateikti informaciją: kam (vardas, pavardė, gyvenamoji vieta) Taryba nusprendė

---

[131] „Klaipėdos apygardos teismo nuosprendis 2019 m. lapkričio 29 d. baudžiamojoje byloje Nr. 1A-185-361/2019“, E-teismai: https://eteismai.lt/byla/189348383075065/1A-185-361/2019?word=teism%C5%B3%20nutartys%20lat

[132] Algimantas Šindeikis, „*Teismų procesinių sprendimų nuasmeninimo konstituncingumo problemos“,* Jurisprudencija, Mykolo romerio universitetas (2009). Prieiga per internetą: https://www.mruni.eu/upload/iblock/76c/3sindeikis.pdf, 43 psl.

[133] *Ibid*, 43 psl.

„leisti parduoti savivaldybei nuosavybės teise priklausančius būstus ir pagalbinio ūkio paskirties pastatą“ bei parduodamų būstų ir pagalbinio ūkio paskirties pastato duomenis[134]. Kitaip tariant pareiškėjas reikalavo jam atskleisti teismo sprendime nurodytą nuasmenintą informaciją, fizinio asmens duomenis. „Pareiškėjas, prašydamas įpareigoti Tarybą pateikti jo prašytą informaciją ir panaikinti skundžiamą Administracijos direktoriaus sprendimą, skundą iš esmės grindė tuo, kad skundžiamame sprendime nenurodyta konkreti Asmens duomenų teisinės apsaugos įstatymo norma, kuri draudžia pateikti prašomą informaciją, kad į Tarybai adresuotą prašymą be pagrindo atsakė Administracijos direktorius. Pareiškėjas skunde vadovavosi Teisės gauti informaciją iš valstybės ir savivaldybių institucijų ir įstaigų įstatymo ir Visuomenės informavimo įstatymo nuostatomis. Pareiškėjas laikėsi pozicijos, kad nuslėpus prašomus pateikti duomenis, privatizavimo procesas tapo neskaidrus, be to, buvo sudarytos sąlygos korupcijos apraiškoms mieste“[135]. Šio ginčo esmė iš principo rodo tai, kad siekiant užtikrinti duomenų apsaugos reikalavimus ir tinkamai nuasmeninti asmens duomenis, gali kilti klausimas ar toks reikalavimas nedaro įtakos skaidrumo principui? Šiuo konkrečiu atveju teismas pasisakė, kad „kadangi pareiškėjas siekia gauti privataus pobūdžio informaciją apie kitus fizinius asmenis bei jų įgytą nuosavybę, tai gali būti daroma tik esant aiškiam teisiniam pagrindui. Teisėjų kolegija sutikdama ir nekartodama pirmosios instancijos teismo skundžiamame sprendime išdėstyto teisinio reglamentavimo, susijusio su asmens duomenų teikimu, ir argumentų, dėl kurių tokie duomenys pareiškėjui negalėjo būti suteikti, papildomai atkreipia dėmesį, kad pats pareiškėjas nenurodė asmenų duomenų gavimo teisinio pagrindo, nors pagal Asmens duomenų teisinės apsaugos įstatymo 6 straipsnį tai turėjo padaryti. Abstraktūs argumentai apie galimą korupciją nesudaro pagrindo pareiškėjui gauti jo prašomą informaciją. Atsižvelgusi į tai, kas išdėstyta, teisėjų kolegija sprendžia, kad pareiškėjas nepagrindė savo skundo reikalavimo ir pirmosios instancijos teismas, išnagrinėjęs teisiškai reikšmingas aplinkybes, pagrįstai nenustatė teisinio pagrindo įpareigoti Tarybą pateikti informaciją: kam (vardas, pavardė, gyvenamoji vieta) Taryba nusprendė „leisti parduoti savivaldybei nuosavybės teise priklausančius būstus ir pagalbinio ūkio paskirties pastatą“ bei parduodamų būstų ir pagalbinio ūkio paskirties pastato duomenis“[136]. Šiuo konkrečiu atveju pareiškėjui nepavyko iš teismo gauti nuasmenintų bylos duomenų dėl to, kad duomenų subjektas neturėjo teisinio pagrindo tokiai informacijai gauti. Tačiau autorius mano, kad tuo atveju, jeigu pareiškėjas turėtų atitinkamą teisinį pagrindą tokiai informacijai gauti, teismo sprendime nuasmeninta informacija galėtų būti jam atskleista. Autorius dar nori atkreipti dėmesį, kad tuo atveju, jeigu teismo sprendime esantys asmens duomenys būtų anonimizuoti, o ne nuasmeninti

[134] „Lietuvos Vyriausiojo administracinio teismo nutartis 2016 m. gruodžio 16 d. byloje Nr. A-3011-520/2016“, E-teismai, https://eteismai.lt/byla/70939150579211/A-3011-520/2016
[135] *Ibid*
[136] *Ibid*

tokiu būdu kaip jie nuasmeninimi pagal Teismo Tarybos nutarimą, pareiškėjas net ir turėdamas teisinį pagrindą gauti atitinkamą informaciją, asmens duomenų nebūtų galėjęs gauti, nes jie būtų anonimizuoti negrįžtamai.

Grįžtant prie klausimo dėl skaidrumo principo teismo procese, Teismo Tarybos nutarimas numato, kad juo be kita ko siekiama užtikrinti ne tik duomenų apsaugos reikalavimų laikymąsi, bet ir teismo proceso skaidrumo principą. Liudvika Meškauskaitė taip pat nurodo, jog „nors teisminio proceso viešumas yra vienas iš pagrindinių principų, tačiau teisminio nagrinėjimo proceso viešumo pobūdis nesuteikia visuomenės informavimo priemonėms absoliučios laisvės skleisti informaciją apie procese dalyvaujančius asmenis ir neatleidžia jų nuo pareigos vertinti teisminių procesų metu gautos informacijos tinkamumo viešinti“[137]. Europos Žmogaus Teisių Teismas byloje Eerikanen v. Finland taip pat buvo pasisakęs, jog aplinkybė, kad privatus asmuo yra teisminio nagrinėjimo subjektas, neįgalina atimti iš tokio asmens teisę į privataus gyvenimo neliečiamumą[138]. Atsižvelgiant į tai autorius mano, kad nuasmeninimas neturėtų daryti įtakos teismo proceso skaidrumo principui.

Svarbu pabrėžti, kad asmens duomenų anonimizavimas ir procesinių dokumentų nuasmeninimas turi ir panašumų. Kaip jau buvo išsiaiškinta anksčiau, asmens duomenų anonimizavimas yra procesas, kuriuo metu iš asmens duomenų yra pašalinami asmens tapatybę galintys atskleisti identifikatoriai. O vienas iš asmens duomenų elementų, kaip jau buvo išsiaiškinta 1.1. skyriuje, yra tas, kad jis nustato fizinio asmens tapatybę. Kaip jau buvo minėta, teismo procesinių sprendimų nuasmeninimas taikomas fizinių asmenų vardui ir pavardei, o kiti asmens duomenys, nurodyti Teismo Tarybos nutarime dėl teismų procesinių sprendimų bei teisėjų drausmės bylose priimtų sprendimų viešo skelbimo tvarkos patvirtinimo tiesiog nėra skelbiami teismo sprendimuose. Atsižvelgiant į tai, autorius pastebi, kad tiek asmens duomenų anonimizavimas, tiek teismo procesinių sprendimų nuasmeninimas yra taikomas fizinių asmenų duomenims. Tačiau verta atkreipti dėmesį, kad Teismo Tarybos nutarimo 12 straipsnis numato išimtinius atvejus, kai nuasmeninami ir juridinių asmenų duomenys; Teismo Tarybos nutarime nurodyta: „juridinių asmenų atstovų, turto administratorių vardai ir pavardės inicialais keičiami, jeigu yra šių asmenų rašytinis prašymas, kuris paduodamas ir išsprendžiamas“. Autorius mano, kad atsižvelgiant į tai, kad 1.1. skyriuje buvo aptariami išimtiniai atvejai, kai asmens duomenimis gali būti pripažinti ir juridinių asmenų duomenys, vadinasi tokiems duomenims išimtiniais atvejais taip pat gali būti taikomas ir asmens duomenų anonimizavimas.

---

[137] Liudvika Meškauskaitė, *„Teisė į privatų gyvenimą“*, Vilnius: Registrų centras, (2015),180 psl.
[138] *Ibid*, 180 psl. Cituota iš EŽTT 2009 vasario 10 d. sprendimas byloje Eerikainen and others v. Finland, peticijos Nr. 3514/02.

Teismo sprendimų nuasmeninimo būtinumas pabrėžia sprendimas byloje Z. V. Finland, kur Teismas konstatavo, jog teismo sprendimo rezoliucinėje dalyje paskelbus visą asmens vardą ir informaciją apie jo sveikatos būklę be asmens sutikimo yra pažeidžiama asmens teisė į privataus gyvenimo gerbimą[139]. Panašiai LAT 2008 m. sausio 2 d. byloje, kuomet viešai paskelbti duomenys apie sūnaus mirtį ir kitas aplinkybes pažeidė asmens teisę į privataus gyvenimo neliečiamumą[140]. Akivaizdu, kad nepageidaujamas asmens duomenų paviešinimas viešoje erdvėje gali sukelti fiziniui asmeniui vienokią ar kitokią žalą. Teismo Tarybos nutarime taip pat yra pabrėžiamas šio proceso tikslas – „užtikrinti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis, nepažeisti asmens duomenų teisinės apsaugos reikalavimų“. Asmens duomenų anonimizavimo tikslas, kaip jau buvo nustatyta anksčiau, yra užtikrinti tinkamą asmens duomenų apsaugą duomenų subjektui, taip pat atitikti asmens duomenų apsaugos reikalavimus. Autorius manymu, šie tikslai yra panašūs, todėl ir šiuo atveju autorius daro prielaidą, kad tai galėtų būti dar vienas asmens duomenų anonimizavimo ir teismo procesinių sprendimų nuasmeninimo panašumas.

Apibendrinant daroma išvada, jog nepaisant to, kad kartais asmens duomenų anonimizavimas, ypač lietuvių kalboje, gali būti vadinamas nuasmeninimu, būtų klaidinga jį tapatinti su teismo procesinių sprendimų ir kitų dokumentų nuasmeninimu. Nuasmeninimas teismo sprendimuose reiškia fizinių asmenų vardų bei pavardžių pakeitimą jų inicialais, jis neužtikrina visiško ir negrįžtamo duomenų anonimiškumo, kaip tai daro asmens duomenų anonimizavimas. Bylos šalių asmens duomenys yra nuasmeninami tik viešai talpinant teismo sprendimus, tačiau originalūs asmens duomenys vis dar išlieka teismo archyvuose, viešai skelbiami teismo posėdžio metu ir teismo skelbimų lentoje. Teismo procesinių sprendimų nuasmeninimas palieka galimybę, nuasmenintus duomenis atskleisti atitinkamą teisinį pagrindą turinčiam asmeniui, tuo tarpu asmens duomenų anonimizavimo atveju, asmeniui net ir turinčiam atitinkamą teisinį pagrindą, asmens duomenys negalėtų būti atskleisti, kadangi jie būtų buvę negrįžtamai anonimizuoti. Verta pabrėžti, kad asmens duomenų anonimizavimas ir teismo procesinių sprendimų nuasmeninimas turi ir panašumų, tokių kaip tikslas atitikti asmens duomenų apsaugos reikalavimus bei tai, kad abu procesai yra nukreipti į fizinių asmens duomenų pašalinimą, tačiau skirtingais būdais.

---

[139] Liudvika Meškauskaitė, *„Teisė į privatų gyvenimą“*, Vilnius: Registrų centras, (2015), 276 psl. Cituota iš EŽTT 1997 m. vasario 25 d. sprendimas byloje Z. v. Finland, peticijos Nr. 9/1996/627/811, paragrafas 113.

[140] „Lietuvos Aukščiausiojo Teismo nutartis 2008 m. sausio 2 d. civilinėje byloje Nr. 3K-7-2/2008, E-teismai: https://eteismai.lt/byla/275755271714690/3K-7-2/2008

3. ASMENS DUOMENŲ ANONIMIZAVIMO METODAI IR JŲ YPATUMAI

3.1. Asmens duomenų anonimizavimo metodai

Atskleidus asmens duomenų anonimizavimo sampratą bei atribojus ją nuo kitų duomenų saugumo priemonių, šiame skyriuje bus atskleidžiama kokiais būdais asmens duomenų anonimizavimas paverčia asmens duomenis anoniminiais bei kaip užtikrinamas duomenų subjektui visiškas anonimiškumas.

Pasak Europos Komisiją, asmens duomenų anonimizavimui būdingi keli anonimizavimo metodai, kurių privalomas standartas Europos Sąjungoje nėra nustatytas[141]. Taip pat Europos Komisija pabrėžia, kad įvairių asmens duomenų anonimizavimo metodo patikimumas yra skirtingas[142]. Atsižvelgiant į tai svarbu nustatyti kokie yra asmens duomenų anonimizavimo metodai ir atskleisti jų turinį.

Skirtingų asmens duomenų anonimizavimo metodų įvairovė rodo tai, kad atitinkamo metodo pasirinkimas priklauso nuo kiekvienos konkrečios situacijos koks tuo atveju metodas yra labiausiai tinkantis[143]. Pavyzdžiui, vienas metodas būtų tinkamas tik apdorojant tiesioginius identifikatorius, kitas metodas – gali būti tinkama priemonė anonimizuojant netiesioginius identifikatorius[144]. Skirtingi asmens duomenų anonimizavimo metodai taip pat skirtingais būdais anonimizuoja asmens duomenis. Kai kurie iš jų keičia tik tam tikras savybes, kai kurie pakeičia kelias savybes, dar kiti pakeičia visas savybes ir įtraukia kitą informaciją, kitaip vadinamą triukšmą. Taip pat kai kuriuos anonimizavimo metodus galima sujungti ir naudoti kartu[145]. Autoriaus manymu, tokia asmens duomenų anonimizavimo metodų įvairovė rodo tai, kad anonimizavimas pasižymi savo pritaikomumu kiekvienai konkrečiai situacijai, taip pat ir lankstumu, kuris suteikia galimybę visakeriopai apsaugoti asmens duomenis nuo galimų duomenų apsaugos pažeidimų. Taip pat galima daryti išvadą, jog šis procesas gali būti naudinga ir lanksti asmens duomenų saugumo priemonė.

„Taikomos duomenų anonimizavimo technikos labai priklauso nuo apdorojamų tekstų pobūdžio ir siekiamo rezultato, taip pat nuo to, kam teikiamas prioritetas – asmens tapatybės anonimiškumo užtikrinimo patikimumui ar teksto teikiamos informacijos išsaugojimui. Taikant kai

---

[141] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 7 psl.
[142] *Ibid*, 12 psl.
[143] Personal Data protection commission Singapore, *„Guide to basic data anonymisation techniques“*, (IAPP, 2018). Prieiga per internetą: https://iapp.org/media/pdf/resource_center/Guide_to_Anonymisation.pdf, 9 psl.
[144] *Ibid*, 9 psl.
[145] *Ibid*, 9 psl.

kurias anonimizavimo technikas ir užmaskavus visą asmens tapatybę atskleisti galinčią informaciją, prarandama ir dalis tyrėjams svarbios informacijos. Taigi technikos pasirinkimas labai svarbus siekiant subalansuoti šiuos du aspektus – užtikrinti, kad būtų apsaugota asmenų tapatybė, kartu paliekant maksimalų kiekį nejautrios informacijos“[146]. Šiuo atveju yra pabrėžiamas vienas iš jau anksčiau aptartų asmens duomenų anonimizavimo trūkumų – tai, kad gali būti ištrinta duomenų valdytojui svarbi informacija arba jos didžioji dalis. Tačiau autorius mano, kad taip pat galima įžvelgti ir privalumą tame, kad egzistuoja keletas asmens duomenų anonimizavimo metodų, kadangi jų įvairovė lemia tai, kad jie skirtingai užtikrina asmens duomenų anonimiškumą ir duomenų valdytojas būtų laisvas rinktis jam tinkamiausią metodą. Atsižvelgiant į tai seka išvada, kad asmens duomenų anonimizavimo metodų įvairovė todėl ir yra reikalinga, kad būtų galimybė priklausomai nuo tuo metu esančios situacijos pasirinkti tokį asmens duomenų anonimizavimo metodą, kuris bus tinkama duomenų saugumo priemonė, tuo pačiu nepažeidžiant duomenų valdytojo siekio išlaikyti jam reikalingą informaciją.

Kaip teigia Balaji Raghunathan, anonimizuoti duomenys tam tikrais atvejais gali būti tikri, realūs duomenys arba gali būti visiškai atsitiktiniai, taip pat gali būti atvejai, kai anonimizavimo išvestis bus kiekvieną kartą vis ta pati reikšmė. Visa tai priklauso nuo to, koks asmens duomenų anonimizavimo metodas konkrečiu atveju bus taikomas[147]. Taigi atsižvelgiant į tai, jog minėti autoriai teigia, kad asmens duomenų anonimizavimo metodų yra keletas ir jų panaudojimą reikia vertinti remiantis tuo metu esančia situacija, šio mokslinio darbo tyrimo prasme svarbu atskleisti šių metodų turinį ir įvertinti, kurį metodą būtų geriausia taikyti vienoje ar kitoje situacijoje. Tačiau kyla klausimas, kokius būtent asmens duomenų anonimizavimo metodus būtų aktualiausia atskleisti?

Valstybinė duomenų apsaugos institucija savo rekomendacijoje dėl nuasmeninimo metodų išskyrė du pagrindinius asmens duomenų anonimizavimo metodus – apibendrinimą ir randomizavimą, nurodydama, kad „asmens tapatybės nustatymo galimybės panaikinimo ir nuasmeninimo metodai yra šiuo metu atliekamų mokslinių tyrimų objektas ir kad tokie tyrimai visuomet parodydavo, jog nėra metodo, kuris neturėtų trūkumų. Plačiąja prasme yra du skirtingi anonimizavimo būdai: pirmasis grindžiamas randomizavimo, antrasis – apibendrinimo principu”[148]. Europos Komisija pasisakydama dėl asmens duomenų anonimizavimo metodų taip pat išskyrė

---

[146] Jūratė Baltrukėnaitė, *„Kokybinių socialinių apklausų anonimizavimo modelis“*, (magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2019). Prieiga per internetą: https://www.vdu.lt/cris/bitstream/20.500.12259/79175/1/Jurate_Baltrukenaite_md.pdf, 20 psl.

[147] Balaji Raghunathan, *„The Complete Book of Data Anonymization – From Planning to Implementation“*, (Taylor & Francis Group, LLC, 2013). http://www.ittoday.info/Excerpts/Data_Anonymization.pdf, 4 psl.

[148] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf, 4 psl.

pagrindinius asmens duomenų anonimizavimo metodus, o tiksliau jų grupes: tai būtų apibendrinimas ir randomizavimas[149].

Siekiant išsiaiškinti kokie iš asmens duomenų anonimizavimo metodų yra dažniausiai naudojami praktikoje, taip pat siekiant parinkti aktualiausius metodus su tikslu juos atkleisti šiame darbe, autorius pasirinko kelias viešai prieinamas privatumo politikas, kuriuose nurodoma, kaip atitinkama bendrovė anonimizuoja asmens duomenys. Atlikus minėtų privatumo politikų paiešką, paaiškėjo, kad tokios žinomos bendrovės kaip Yahoo[150], Apple[151], Orange[152], Airbnb[153] nepaisant to, kad nurodo savo privatumo politikose, jog asmens duomenis anonimizuoja, jos nedetalizuoja kokius konkrečius asmens duomenų anonimizavimo metodus yra pasirinkusios taikyti. Todėl atsižvelgiant į tai, autorius pasirinko tik dviejų plačiai žinomų bendrovių privatumo politikas, kuriose buvo aiškiai nurodyta kokius asmens duomenų anonimizavimo metodus jos taiko: 1) bendrovė – Google ir 2) Instagram. Toliau bus plačiau aptariama kokius konkrečius duomenų anonimizavimo metodus yra pasirinkusios taikyti šios bendrovės.

Pirmiausia buvo aiškinamasi kaip Google anonimizuoja asmens duomenis. Google – yra pasaulyje plačiai žinomas paieškos portalas, internetinė reklamavimosi platforma[154]. Google privatumo politika yra viešai paskelbta ir duomenų subjektai be apribojimų ir jiems suprantama kalba gali susipažinti, be kita ko, su informacija, kaip yra anonimizuojami jų duomenis[155]. Pirmiausia Google savo privatumo politikoje apibrėžia kas yra asmens duomenų anonimizavimas: „anonimizavimas yra duomenų apdorojimo technologija, kurią taikant asmens identifikavimo informacija pašalinama arba pakeičiama; todėl anonimizuoti duomenys negali būti susieti su jokiu asmeniu. Taip pat tai yra labai svarbus „Google“ privatumo įsipareigojimo komponentas“[156]. Toliau Google pateikia paaiškinimą kokiu tikslu jis atitinkamų duomenų subjektų duomenis anonimizuoja: „analizuodami anonimizuotus duomenis galime kurti saugius ir vertingus produktus bei funkcijas, pvz., įvestos paieškos užklausos automatinį užbaigimą, ir geriau aptikti saugos grėsmes, pvz., sukčiavimo ir kenkėjiškas svetaines, tuo pačiu apsaugodami naudotojų tapatybes. Taip pat galime

---

[149] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 7 psl.

[150] „Yahoo privatumo politika“ žiūrėta 2019 m. spalio 30 d. Prieiga per internetą: https://policies.yahoo.com/ie/en/yahoo/privacy/index.htm?redirect=no

[151] *„Apple privatumo politika“*, žiūrėta 2019 m. spalio 30 d. Prieiga per internetą: https://www.apple.com/legal/privacy/en-ww/

[152] „*Orange privatumo politika“*, žiūrėta 2019 m. spalio 30 d. Prieiga per internetą: https://www.orange-business.com/sites/default/files/obs-privacy-policy-customers-and-prospects_oct-2019.pdf#chapter8

[153] *„Airbnb privatumo politika”*, žiūrėta 2019 m. spalio 30 d. Preiga per internetą: https://www.airbnb.com/terms/privacy_policy

[154] Vikipedija, *„Google*“, žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://lt.wikipedia.org/wiki/Google

[155] *Google privatumo politika, „Kaip „Google“ anonimizuoja duomenis“*, žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://policies.google.com/technologies/anonymization?hl=lt

[156] *Ibid*

saugiai bendrinti anonimizuotus duomenis išorinėse sistemose, todėl jie yra naudingi kitiems žmonėms“[157]. Toliau Google aptaria ir plačiau paaiškina jo taikomus anonimizavimo metodus. Šiuo atveju Google yra pasirinkusi 2 anonomizavimo metodus, siekiant apsaugoti duomenų subjektų duomenis, tai būtų: 1) duomenų apibendrinimas ir 2) triukšmo pridėjimas prie duomenų arba diferencinis privatumas[158].

Kita tyrima bendrovė buvo Instragram. Tai yra taip pat plačiai žinomas, nuotraukų ir kitų vaizdinio turinio dalinimosi socialinis tinklas[159]. Ši bendrovė savo viešai paskelbtoje privatumo politikoje taip pat nurodo, kad jie siekiant užtikrinti tinkamą duomenų apsaugą duomenis anonimizuoja[160]. Tačiau palyginus šią privatumo politiką su Google privatumo politika, Instagram ne taip plačiai pateikia informaciją apie asmens duomenų anonimizavimą. Pirmiausia ši bendrovė nepateikia asmens duomenų anonimizavimo apibrėžimo ar kitokio paaiškinimo kas yra anonimizavimas, taip pat Instagram nedetalizuoja kokius konkrečius duomenų kategorijas ir kokiems tikslams jie duomenis anonimizuoja. Šios bendrovės privatumo politikoje nurodoma, kad jie gali pašalinti dalį tam tikrų duomenų, kurie gali asmenį identifikuoti ir taip pat nurodo, jog jie gali sujungti vieną informaciją su kita, tokiu būdu ją anonimizuojant, kad ji nebebūtų susijusi su konkrečiu asmeniu ir atlikus šį veiksmą tvarkyti tik apibendrintą informaciją[161]. Iš viešai pateiktos informacijos, galima daryti išvadą, jog ši bendrovė yra pasirinkusi bent vieną asmens duomenų anonimizavimo metodą ir iš pateikto apibrėžimo, panašu, kad tai būtų apibendrinimas.

Taigi, atsižvelgiant į tai, kad tiek Valstybinė duomenų apsaugos institucija, tiek Europos Komisijos darbo grupė savo rekomendacijose nurodo, jog iš keletos asmens duomenų anonimizavimo metodų plačiausiai naudojami ir dažniausiai pasitaikantys praktikoje yra randomizavimas ir apibendrinimas. Taip pat atsižvelgiant į tai, kad tokios plačiai žinomos bendrovės kaip Instagram ir Google savo privatumo politikose taip pat išskiria būtent šiuos asmens duomenų anonimizavimo metodus, autorius daro prielaidą, kad randomizavimas ir apibendrinimas yra plačiausiai naudojami asmens duomenų anonimizavimo metodai, todėl būtent jų turinius būtų aktualiausia atskleisti šiame moksliniame darbe.

---

[157] *Google privatumo politika, „Kaip „Google“ anonimizuoja duomenis“*, žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://policies.google.com/technologies/anonymization?hl=lt
[158] *Ibid*
[159] Vikipedija, *„Instagram*“, žiūrėta 2019 spalio 30 d. Prieiga per internetą: https://lt.wikipedia.org/wiki/Instagram
[160] *„Instagram privatumo politika“*, žiūrėta 2019 spalio 30 d. Prieiga per internetą: https://help.instagram.com/402411646841720
[161] *Ibid*

3.1.1. Randomizavimo metodai

Europos Komisija nuomonėje dėl nuasmeninimo metodų pateikia pirmosios asmens duomenų anonimizavimo metodų grupės – randomizavimo apibrėžimą[162]. „Randomizavimas – tai metodų, kuriais keičiamas duomenų tikrumas siekiant panaikinti aiškią duomenų ir asmens sąsają, grupė. Kai duomenys yra ganėtinai nekonkretūs, jų nebegalima susieti su konkrečiu asmeniu. Taikant randomizavimą, atskirų įrašų savitumas nemažėja, nes kiekvienas įrašas vis viena bus išvedamas pagal atskirą duomenų subjektą, tačiau šiuo būdu užtikrinama apsauga nuo išvestinės informacijos gavimo išpuolių ir (arba) rizikos ir jį, siekiant suteikti didesnę privatumo garantiją, galima derinti su apibendrinimu. Norint užtikrinti, kad remiantis įrašu, nebūtų galima nustatyti pavienio asmens tapatybės, gali prireikti papildomų metodų“[163]. Kitaip tariant randomizavimas pasireiškia tikrųjų verčių pakeitimu siekiant panaikinti galimybę nuasmenintus duomenis susieti su pirminėmis vertėmis[164]. Remiantis minėta Europos Komisijos nuomone, randomizavimui būdingi 3 anonimizavimo metodai: 1) iškraipytų duomenų įterpimas, 2) perstatymas ir 3) diferencinis privatumas[165].

Pirmasis šiame darbe aptariamas randomizavimo grupės metodas bus iškraipytų duomenų įterpimas. Pasak Europos Komisiją, šis metodas „pirmiausia naudingas tada, kai požymiai gali turėti reikšmingą neigiamą poveikį asmenims. Šio metodo esmė – į duomenų rinkinį įtrauktų požymių pakeitimas sumažinant jų tikslumą, tačiau išsaugant bendrą pasiskirstymą. Tvarkydamas duomenų rinkinį, stebėtojas manys, kad vertės yra tikslios, bet tai bus teisinga tik iš dalies. Pavyzdžiui, jeigu asmens ūgis iš pradžių buvo išmatuotas centimetrų tikslumu, anonimizuotame duomenų rinkinyje ūgis gali būti nurodomas tik ±10 cm tikslumu. Jeigu šis metodas bus taikomas veiksmingai, trečioji šalis negalės nustatyti asmens tapatybės ir neturėtų galėti ištaisyti duomenis arba kaip nors kitaip nustatyti, kaip duomenys buvo pakeisti. Iškraipytų duomenų įterpimą paprastai reikia derinti su kitais nuasmeninimo metodais, pvz., su akivaizdžių požymių ir kvaziindentifikatorių pašalinimu. Iškraipymo laipsnis turėtų priklausyti nuo to, kokio lygio informacija yra reikalinga, ir nuo apsaugotų požymių atskleidimo daromo poveikio asmenų privatumui“[166]. Žinomi leidėjai valdantys didelį mąstą asmens duomenų dažnai naudoja iškraipytų duomenų įterpimų metodą su tikslu pašalinti identifikatorius, tačiau tai darydami jie gali prarasti nemažą kiekį duomenų, ko pasekoje apdorotų duomenų paskelbimas tampa beprasmis. Atsižvelgiant į tai yra nuolat ieškomas

---

[162] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 12-13 psl.
[163] *Ibid*, 12-13 psl.
[164] *Ibid*, 29 psl.
[165] *Ibid*, 13-15 psl.
[166] *Ibid*,13 psl.

balansas tarp privatumo ir naudos gavimo[167]. Taigi, iškraipytų duomenų įterpimo metodas pasireiškia asmens duomenų tikslumo sumažinimu įterpiant taip vadinamąjį „triukšmą“, tuo pačiu išsaugant duomenų bendrą pasiskirstymą.

Kitas randomizavimo grupės metodas yra perstatymas[168]. „Taikant šį metodą, požymių vertės sukeičiamos vietomis taip, kad kai kurios iš jų būtų dirbtinai susietos su kitais duomenų subjektais. Tai naudinga, kai svarbu išsaugoti tikslų kiekvieno į duomenų rinkinį įtraukto požymio pasiskirstymą. Perstatymas gali būti laikomas savita iškraipytų duomenų įterpimo rūšimi. Pagal klasikinį iškraipytų duomenų įterpimo metodą požymiai pakeičiami pasirenkant atsitiktines vertes. Dėsningai iškraipytų duomenų įterpimas gali būti sunkiai įvykdomas uždavinys, o nedaug pakeičiant požymių vertes gali būti neužtikrintas pakankamas privatumas. Perstatymo metodas – tai alternatyva, kurią taikant duomenų rinkinio vertės pakeičiamos tiesiog sumaišant vietomis skirtingų įrašų vertes. Tokiu sukeitimu užtikrinama, kad verčių intervalas ir paskirstymas išliktų tokie patys, o verčių ir asmenų koreliacijos pasikeistų. Jeigu dviem arba daugiau požymių būdingas loginis tarpusavio ryšys arba statistinė koreliacija ir atliekamas nepriklausomas jų perstatymas, toks ryšys sunaikinamas. Todėl gali būti svarbu susijusių požymių rinkinio perstatymą atlikti taip, kad nebūtų pažeistas loginis tarpusavio ryšys, nes kitaip išpuolio vykdytojas galėtų nustatyti sukeistus požymius ir atlikti atvirkštinį perstatymą. Tarkime, medicinos duomenų rinkinyje yra požymių poaibis „hospitalizavimo priežastys, simptomai, atsakingas skyrius“; dažniausiai tarp šių verčių bus stiprus loginis ryšys, todėl, atlikus tik vienos iš šių verčių perstatymą, ją bus galima nustatyti ir gal netgi atlikti atvirkštinį perstatymą. Panašiai kaip ir iškraipytų duomenų įterpimo atveju, vien perstatymo pritaikymas gali neužtikrinti nuasmeninimo, todėl jis visada turėtų būti derinamas su akivaizdžių požymių ir (arba) kvaziidentifikatorių pašalinimu“[169]. Taigi, šio metodo esmė yra ta, kad tam tikri duomenys yra sukeičiami vietomis taip, kad būtų neįmanoma nustatyti kokiam konkrečiam duomenų subjektui jie priklauso.

Ir trečiasis randomizavimo grupės metodas yra diferencinis privatumas[170]. „Diferencinis privatumas priskiriamas randomizavimo metodų grupei, tačiau jis pagrįstas kitokiu principu: iškraipytų duomenų įterpimas taikytinas prieš paskelbiant duomenų rinkinį, o diferencinio privatumo metodas gali būti taikomas, kai duomenų valdytojas parengia nuasmenintus duomenų rodinius, išsaugodamas pirminių duomenų kopiją. Tokie nuasmeninti rodiniai paprastai parengiami

---

[167] Kato Mivule, *„Utilizing noise addition for data privacy, an overview“*, (Bowie State University, 2013). Prieiga per internetą: https://arxiv.org/pdf/1309.3958.pdf, 1 psl.
[168] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 13 psl.
[169] *Ibid*, 13 psl.
[170] *Ibid*, 15 psl.

naudojant užklausų poaibį, skirtą tam tikrai trečiajai šaliai. Į šį poaibį vėliau sąmoningai įtraukiami atsitiktiniai iškraipyti duomenys. Taikydamas diferencinio privatumo metodą, duomenų valdytojas sužino, kiek iškraipytų duomenų jis turėtų įterpti ir kokiu pavidalu, kad užtikrintų reikiamas privatumo garantijas. Šiuo atveju labai svarbu nuolat stebėti (ne rečiau kaip kiekvienos naujos užklausos atveju), ar neatsirado galimybė nustatyti asmens tapatybę pasinaudojant užklausos rezultatų aibe. Be to, derėtų paaiškinti, kad diferencinio privatumo metodu pirminiai duomenys nepakeičiami, o kol jie išlieka, duomenų valdytojas, atsižvelgdamas į visas galimas pasitelktinas priemones, asmens tapatybę gali nustatyti pasinaudodamas diferencinio privatumo užklausų rezultatais. Šie rezultatai taip pat turėtų būti laikomi asmens duomenimis. Vienas iš diferenciniu privatumu pagrįsto metodo privalumų yra tas, kad duomenų rinkiniai įgaliotosioms trečiosioms šalims teikiami pagal konkrečias užklausas, o ne paskelbiant visą duomenų rinkinį. Kad būtų lengviau atlikti auditą, duomenų valdytojas gali išsaugoti visų užklausų ir prašymų sąrašą, taip užtikrindamas, kad trečiosios šalys negautų duomenų, su kuriais jos neturi teisės susipažinti. Be to, norint geriau apsaugoti privatumą, užklausai gali būti taikomi kiti nuasmeninimo, pvz., iškraipytų duomenų įterpimo arba pakeitimo, metodai. Tyrinėtojams dar nepavyko sukurti gero interaktyvaus užklausų ir jų rezultatų teikimo mechanizmo, kurį naudojant būtų galima ir gana tiksliai (t. y. kuo mažiau iškraipant duomenis) atsakyti į visas užklausas, ir apsaugoti privatumą. Siekiant apriboti išvados padarymo ir susiejimo išpuolių galimybę, būtina sekti subjektų teikiamas užklausas ir stebėti apie duomenų subjektus gautą informaciją; todėl diferencinio privatumo metodu valdomos duomenų bazės neturėtų būti prieinamos viešoms paieškos sistemoms, kuriose nėra užklausas teikiančių subjektų sekimo galimybės“[171].

Kaip jau buvo išsiaiškinta anksčiau, diferencinį privatumą taiko Google, anonimizuojant jo vartotojų asmens duomenis[172]. Google savo privatumo politikoje be kita ko pateikia diferencinio privatumo metodo taikymo pavyzdį: kai matuojama bendra paieškų gripo tema tendencija visame geografiniame regione, prie duomenų rinkinio yra pridedamas „triukšmas“, kitaip tariant jie gali pridėti arba atimti tam tikrą žmonių, ieškančių informacijos apie gripą nurodytoje kaimynystėje, skaičių, bet taip, kad tai niekaip nepaveiktų tendencijos matavimų didesniame geografiniame regione[173]. Europos Komisija taip pat pažymi, kad „iškraipyti duomenys įterpiami siekiant dviejų pagrindinių tikslų: pirma, norint apsaugoti į duomenų rinkinį įtrauktų duomenų

[171] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 15-16 psl.
[172] *Google privatumo politika, „Kaip „Google“ anonimizuoja duomenis“*, žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://policies.google.com/technologies/anonymization?hl=lt
[173] *Ibid*

subjektų privatumą, antra, norint išsaugoti paskelbtos informacijos naudingumą“[174]. Taigi, diferencinio privatumo metodas pasireiškia duomenų iškraipymų įterpiant kitą informaciją į duomenų rinkinį, tačiau palyginus su iškraipytų duomenų įterpimo metodu, diferencinio privatumo metodas taikomas tik tuo atveju, jeigu yra pateikiama tokio duomenų rinkinio parengimo užklausą, todėl siekiant užtikrinti tinkamą šio metodo taikymą, duomenų valdytojas turėtų sekti ir atsižvelgti į ankstesnes užklausas, kad išvengtų duomenų susiejimo rizikos.

Svarbu pabrėžti, kad praktikoje pasitaiko netinkamų šių metodų taikymo pavyzdžių. Europos Komisija jau minėtoje savo nuomonėje dėl nuasmeninimo metodų pateikia tikrą pavyzdį, kaip netinkamai gali būti taikomas randomizavimas. „Gerai žinomas netinkamai nuasmeninto duomenų rinkinio paskelbimo atvejis, susijęs su Netflix Prize. Išnagrinėjus tipinį įrašą duomenų bazėje, kurioje buvo randomizuota keletas su duomenų subjektu susijusių požymių, matyti, kad kiekvieną įrašą vis dar galima padalyti į du smulkesnius įrašus, t. y. randomizuoti požymiai, aiškūs požymiai, šiuo atveju aiškiu požymiu gali būti bet koks tariamai ne asmens duomenų derinys. Konkreti išvada, kurią galima padaryti remiantis Netflix Prize duomenų rinkiniu, gauta pastebėjus, kad kiekvieną įrašą galima pažymėti kaip tašką daugiamatėje erdvėje, kurioje kiekvienas aiškus požymis yra atskira koordinatė. Pagal šį principą bet koks duomenų rinkinys gali būti laikomas taškų aibe tokioje daugiamatėje erdvėje, kuriai gali būti būdingas labai mažas tankis, o tai reiškia, kad taškai gali būti labai nutolę vienas nuo kito. Išties jie gali būti taip toli vienas nuo kito, kad, erdvę padalijus į plačias sritis, kiekvienoje liks tik po vieną įrašą. Net ir įterpus iškraipytų duomenų, įrašai nepriartėja vienas prie kito tiek, kad patektų į tą pačią daugiamatę sritį“[175]. „Pavyzdžiui, atliekant su Netflix susijusį eksperimentą, įrašai, kurie apėmė tik aštuonis filmų įvertinimus, kuriuos skiria 14 dienų, buvo pakankamai unikalūs. Į įvertinimus ir datas įterpus iškraipytų duomenų, sričių sutapimo nepastebėta. Kitaip tariant, pasirinkus tik aštuonis įvertintus filmus, nustatytas visoje duomenų bazėje tarp jokių dviejų duomenų subjektų nesikartojantis pareikštų įvertinimų bruožas. Remdamiesi šia geometrine išvada, tyrinėtojai tariamai anoniminį Netflix duomenų rinkinį palygino su kita vieša filmų vertinimo duomenų baze (IMDb) ir nustatė naudotojus, kurie tokiais pat laikotarpiais įvertino tuos pačius filmus. Kadangi daugumą naudotojų buvo galima unikaliai susieti tarpusavyje, iš IMDb duomenų bazės gautą pagalbinę informaciją buvo galima importuoti į paskelbtą Netflix duomenų rinkinį ir taip visus tariamai nuasmenintus įrašus papildyti tapatybės duomenimis. Svarbu pažymėti, kad tai – bendra savybė: likusi bet kokios randomizuotos duomenų bazės dalis išlaiko labai didelę galimybę pagal ją nustatyti asmens tapatybę; ši galimybė priklauso nuo liekamųjų požymių derinių retumo. Šį svarbų aspektą duomenų valdytojai, pasirinkdami randomizavimą, kaip reikiamo nuasmeninimo

[174] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 30 psl.
[175] *Ibid*

lygio pasiekimo būdą, visada turėtų turėti omenyje.“[176]. Taigi šis pavyzdys rodo, kad randomizavimo metodų grupei būdinga tapatybės nustatymo rizika, ypač tuo atveju, jeigu duomenų valdytojas ne iki galo tinkamai parinks ir taikys vieną ar kelis randomizavimo metodus, todėl duomenų valdytojams rekomenduojama rinktis kelis anonimizavimo metodus ir derinti juos tapusavyje, kad būtų pasiektas tinkamas galutinis rezultatas – visiškas duomenų anonimizavimas.

Apibendrinant, randomizavimas yra grupė asmens duomenų anonimizavimo metodų į kurį įeina 3 metodai: 1) iškraipytų duomenų įterpimas, kuris pasireiškia duomenų tikslumo sumažinimu įterpiant atsitiktinę informaciją arba kitaip vadinamą triukšmą, tuo pačiu išsaugant bendrą duomenų paskirstymą; 2) perstatymas, kuris pasireiškia duomenų sukeitimu tokiu būdu, kad jie nebegalėtų būti priskirti konkrečiam duomenų subjektui; ir 3) diferencinis privatumas, kuris taip pat pasireiškia duomenų iškaipymų, įterpiant atsitiktinę informaciją, tačiau yra taikomas tik pagal atskiras užklausas, kurios taip pat turi būti fiksuojamos, siekiant išvengti duomenų susiejimo galimybes. Kiekvieno šio metodo netinkamas parinkimas ir (ar) taikymas gali lemti duomenų subjekto tapatybes nustatymą, ko pasekoje asmens duomenų anonimizavimas nebus veiksminga duomenų saugumo priemonė. Be to pastebėtina, kad šios grupės metodai ne visais atvejais gali užtikrinti visišką asmens duomenų anonimizavimą, todėl duomenų valdytojams rekomenduojama derinti kelis asmens duomenų anonimizavimo metodus tarpusavyje.

3.1.2. Apibendrinimo metodai

Kita asmens duomenų anonimizavimo metodų grupė yra apibendrinimas[177]. „Pagal šį principą duomenų subjektų požymiai apibendrinami arba, kitaip tariant, susilpninami, kiek pakeičiant atitinkamą mastelį arba dydžio eilę (pvz., informaciją pateikiant ne miesto, o regiono mastu, mėnesio, o ne savaitės apimtimi). Nors apibendrinimas, siekiant panaikinti išskyrimo galimybę, ir gali būti veiksmingas, ne visais atvejais šiuo principu užtikrinamas tinkamas anonimizavimas; pirmiausia, taikant šį principą, būtina pasitelkti specialius sudėtingus kiekybinius metodus, kuriais būtų panaikinta susiejimo ir išvados padarymo galimybė“[178]. Apibendrinimas yra skirstomas į kelis metodus: 1) agregavimas ir k anonimiškumas ir 2) l įvairovė ir t tankis[179].

---

[176] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 32 psl.
[177] *Ibid*, 17 psl.
[178] *Ibid*, 17 psl.
[179] *Ibid*, 17 psl.

Visų pirma, bus atskleidžiamas agregavimo ir k anonimiškumo metodų turinys. „Agregavimo ir k anonimiškumo metodais siekiama panaikinti galimybę išskirti duomenų subjektus, juos grupuojant kartu su ne mažiau kaip k kitų asmenų. Šiuo tikslu požymių vertės apibendrinamos tokiu mastu, kad kiekvienam asmeniui būtų priskirta tokia pat vertė. Pavyzdžiui, vietovės mastelį pastambinus nuo miesto iki šalies, bus įtraukta daugiau duomenų subjektų. Pavienių asmenų gimimo datos gali būti apibendrintos datų intervalais arba sugrupuotos pagal mėnesius arba metus. Kitus skaitinius požymius (pvz., darbo užmokestį, svorį, ūgį, vaisto dozę) galima apibendrinti verčių intervalais (pvz., darbo užmokestis nuo 20 000 iki 30 000 EUR). Šie metodai gali būti taikomi tada, kai dėl požymių tikslių verčių koreliacijos gali susidaryti kvaziindikatoriai"[180].

Duomenų agregavimas, kaip vienas iš apibendrinimo grupės metodų, yra apibrėžiamas kaip procesas, kuriuo metu yra apibendrinami skirtingi asmens duomenys, siekiant pašalinti perteklinius identifikatorius, kurie gali lemti asmens tapatybės nustatymą[181]. Agregavimas apibendrina pačius svarbiausius asmens duomenis, pašalinant nedidelę dalį duomenų iš lenteles, kad jie galėtų būti saugiai prieinami viešai[182]. Europos Komisija nuomonėje dėl nuasmeninimo metodų buvo pateikusi duomenų agregavimo pavyzdį: 8 asmenims, kurie yra iš 8 skirtingų miestų buvo priskirtos 2 savybės (P1 ir P2)[183]. Siekiant apsunkinti duomenų susiejimą, duomenų valdytojas gali pakeisti arba tiksliau tariant apibendrinti duomenis apie asmenų gyvenamuosius miestus į šalį ir tokiu būdu, žmonės gyvenantys Milane ir Rome bus apibendrinami ir prie jų bus nurodoma, kad jie gyvena Italijoje. Tokiu būdu bus sunkiau nustatyti konkretų asmenį, tačiau tuo atveju, jeigu asmuo iš visos grupės asmenų yra tik vienas iš tam tikros šalies, toks duomenų apibendrinimas, pavyzdžiui kaip iš Paryžiaus į Prancuziją, duomenų susiejimo rizikos nesumažina, nes asmuo vis dar lieka nesunkiai identifikuojamas. Atsižvelgiant į tai, Europos Komisija atkreipia dėmesį, „kad visais atvejais, kai duomenys yra išsklaidyti (pvz., geografinėje vietovėje tam tikra savybė būdinga tik keletui asmenų) ir kai, atliekant pirminį duomenų agregavimą, jų negalima sugrupuoti taip, kad skirtingos savybės kartotųsi pakankamai dažnai (pvz., geografinėje vietovėje keletas savybių gali kartotis retai), norint pasiekti reikiamą nuasmeninimo lygį, gali prireikti atlikti papildomą agregavimą"[184]. Tokiu atveju duomenų valdytojas galėtų duomenis apibendrinti dar plačiau, pavyzdžiui iki žemyno, tačiau ir tokiu atveju tai ne visada gali būti veiksminga priemonė, be to ji gali būti ne tiek naudinga, nes labai plačiai

[180] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų"*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 18 psl.
[181] Miguel Antonio ir kt., „*Intelligent Data Sensing and Processing for Health and Well-being Applications"*, (Elsvier, 2018), 42 psl.
[182] *Ibid*, 42 psl.
[183] Europos Komisija, *op.cit.*, 34 psl.
[184] *Ibid*, 38 psl.

apibendrinant duomenis, duomenų valdytojas gali prarasti didelę dalį jam naudingų duomenų[185]. Šioje vietoje verta pabrėžti, kad duomenų valdytojams labai svarbu išsaugoti kuo daugiau jam naudingos informacijos[186].

Autorius, siekdamas plačiau atskleisti agregavimo metodą, remdamasis Europos Komisijos nuomone dėl nuasmeninimo metodų, pateikia iliustracinį pavyzdį A lentelėje, kaip agregavimo metodas gali būti taikomas praktikoje:

A lentelė. Asmens duomenų anonimizavimo metodas – agregavimas

Asmens tapatybės numeris	Vietovės kodas	Savybė
1.	Roma	P1
2.	Madridas	P1
3.	Londonas	P2
4.	Paryžius	P1
5.	Barselona	P1
6.	Milanas	P2
7.	Niujorkas	P2
8.	Berlynas	P1

Asmens tapatybės numeris	Vietovės kodas	Savybė
1.	Italija	P1
2.	Ispanija	P1
3.	Jungtinė Karalystė	P2
4.	Prancūzija	P1
5.	Ispanija	P1
6.	Italija	P2
7.	JAV	P2
8.	Vokietija	P1

[187]

Kairėje A lentelės pusėje yra nurodyti tokie duomenys kaip asmens tapatybės numeris, vietovės kodas ir tam tikra priskirta savybė, šie duomenys pateikti iki agregavimo proceso. Dešinėje lentelės pusėje yra tie patys duomenys, tačiau jau po agregavimo. Kaip galima matyti, bei kaip jau buvo aptarta anksčiau, siekiant sumažinti duomenų susiejimo galimybę, konkretaus duomenų subjekto miestas buvo pakeistas į platesnį duomenį – į šalį. Tačiau autorius pastebi, kad ko gero tai nebus geriausias agregavimo pavyzdys, kadangi keturių duomenų subjektų susiejimo rizika išliko nesumažinta. Šių duomenų subjektų vertė šioje lentelėje buvo unikali iš pat pradžių, t.y. vienintelis asmuo iš Londono, ar Paryžiaus, ar Niujorko ar Berlyno, ir po agregavimo situacija nepakito, jis išliko

[185] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 34-36 psl.
[186] Miguel Antonio ir kt., „*Intelligent Data Sensing and Processing for Health and Well-being Applications“*, (Elsvier, 2018), 42 psl.
[187] Europos Komisija, *op.cit.*, 34-35 psl.

unikalus. Šiuo atveju apibendrinant duomenis nuo miestų iki šalies tokio asmens unikalumas pateiktoje lentelėje neišnyko, jis vis dar liko vienintelis iš konkrečios šalies.

K anonimiškumas taip pat yra apibendrinimo grupės metodas[188]. K anonimiškumas laikomas paprastu, bet praktišku asmens duomenų anonimizavimo metodu, kuris užtikrina duomenų subjektų konfidencialumą[189]. Šis metodas garantuoja, kad visi įrašai lentelėje yra tikri ir susiję su lentelėje esančiais duomenų subjektais, bet tuo pačiu yra konfindencialūs. Be to k anonimiškumas užtikrina, kad jokia informacija apie duomenų subjektus nebus panaikinta, o bus atspindėta lentelėje[190]. Pavyzdžiui, jeigu duomenų rinkinyje yra tik vienas vyresnis nei šimtą metų vyras iš Tamperės, šis asmuo turėtų būti suskirstytas į kitas grupes, kad jis nebūtų vienintelis asmuo, turintis šiuos požymius. Jei duomenų rinkinyje yra kitų vyrų, vyresnių nei 90 metų iš Tamperės, šimtametį vyrą būtų galima paskirstyti į tą grupę[191]. Tiksli k reikšmė nėra nustatyta, todėl ji turėtų būti sprendžiama kiekvienu konkrečiu atveju. Kartais gali pakakti dviejų duomenų vienetų k, tačiau pirmenybė teikiama mažiausiai trims. Kai kurie mokslininkai teigia, kad k turėtų būti 5 – 10 duomenų vienetų[192].

Siekiant geriau suprasti šio metodo veikimo mechanizmą, B lentelėje pateikiamas pavyzdys kokiu būdu asmens duomenys anonimizuojami k anonimiškumo metodu pagalba:

B lentelė. Asmens duomenų anonimizavimo metodas – k anonimiškumas

	QI_1	QI_2	S_1
ID	Age	Zip	Disease
1	5	15	Flu
2	15	25	Fever
3	28	28	Diarrhea
4	25	15	Fever
5	22	28	Flu
6	32	35	Fever
7	38	32	Flu
8	35	25	Diarrhea

	QI_1	QI_2	S_1
ID	Age	Zip	Disease
1	0-20	10-30	Flu
2	0-20	10-30	Fever
3	20-30	10-30	Diarrhea
4	20-30	10-30	Fever
5	20-30	10-30	Flu
6	30-40	20-40	Fever
7	30-40	20-40	Flu
8	30-40	20-40	Diarrhea

[193]

[188] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 36-37 psl.
[189] Reda Alhajj, Hong Gao, Xue Li, Jianzhong Li, Osmar R. Zaiane, *„Advanced Data Mining and Applications“*. (Springer, 2017), 89 psl.
[190] *Ibid*, 89 psl.
[191] Finnish social science data archive, *„Anonymisation and personal data“*, žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://www.fsd.uta.fi/aineistonhallinta/en/anonymisation-and-identifiers.html
[192] *Ibid*
[193] Zahid Pervaiz, Walid G. Aref, Arif Ghafoor, Nagabhushana Prabhu, *„Accuracy-Constrained Privacy-Preserving Access Control Mechanismfor Relational Data“*, (Research gate, 2014). Prieiga per internetą: https://www.researchgate.net/publication/261567414_Accuracy-Constrained_Privacy-Preserving_Access_Control_Mechanismfor_Relational_Data, 3 psl.

Iš pateiktos lentelės galima matyti, kad kairėje pusėje nurodyti duomenys yra iki apdorojimo, tai yra pirminiai duomenų subjektų duomenys. Šioje lentelėje yra pateikti toliau išvardinti duomenys: identifikacinis (ID) numeris, asmens amžius (Age), pašto kodas (Zip) ir liga (disease). Dešinėje lentelėje nurodyti jau apibendrinti asmens duomenis. Kaip matome, buvo apibendrintas asmenų amžius ir suskirstytas į 3 grupės: nuo 0 iki 20, nuo 20 iki 30 ir nuo 30 iki 40. Taip pat buvo apibendrintas pašto kodas ir jis buvo susikirstytas į 2 grupes: nuo 10 iki 30 ir nuo 20 iki 40. Labai svarbus aspektas, kad net ir po duomenų apdorojimo, jokie duomenys iš lentelės nebuvo panaikinti, jie vis dar išliko joje, tačiau ne tiek tikslūs kokie jie buvo iki anonomizavimo.

Būtina pridėti, kad „k anonimiškumo metodas parengtas remiantis pakartotinio tapatybės nustatymo eksperimentu, atliktu pačioje XX a. pabaigoje, kai privati JAV sveikatos priežiūros įmonė viešai paskelbė neva nuasmenintą duomenų rinkinį. Nuasmeninimas atliktas pašalinus subjektų vardus ir pavardes, bet duomenų rinkinyje buvo palikti su sveikata susiję duomenys ir kiti požymiai, pvz., pašto (gyvenamosios vietos) kodas, lytis ir visa gimimo data. Tie patys trys elementai (pašto kodas, lytis, visa gimimo data) yra įtraukti ir į kitus viešuosius registrus (pvz., rinkėjų sąrašą), todėl akademinis tyrinėtojas, naudodamasis šiais duomenimis, konkrečių duomenų subjektų tapatybę galėjo susieti su paskelbto duomenų rinkinio požymiais. Išpuolio vykdytojas (tyrinėtojas) galėjo turėti tokių bendrųjų žinių: „žinau, kad į rinkėjų sąrašą įtrauktas duomenų subjektas, kuriam priskirti trys konkretūs elementai (pašto kodas, lytis, visa gimimo data), yra unikalus. Paskelbtame duomenų rinkinyje yra šių trijų požymių įrašas.“ Atlikus empirinį tyrimą, nustatyta, kad absoliučią daugumą (daugiau kaip 80 proc.) duomenų subjektų, įtrauktų į viešąjį registrą, kuriuo buvo naudojamasi per šį eksperimentą, buvo galima vienareikšmiškai susieti su konkrečiu trijų elementų rinkiniu, todėl buvo galima nustatyti ir asmenų tapatybę. Taigi šiuo atveju duomenys buvo nuasmeninti netinkamai”[194]. Autorius mano, kad šiuo pavyzdžiu siekiama atkreipti dėmesį, kad k anonimiškumas, kaip ir kiti prieš tai aptarti anonimizavimo metodai taip pat gali kelti asmens tapatybės nustatymo riziką, ypač tuo atveju, kai yra netinkamai pritaikytas minėtas metodas.

Apibendrinimo metodų grupė neapsiriboja vien tik agregavimo ir k anonimiškumo metodais, ši grupė taip pat turi ir kitus anonimizavimo metodus, tokius kaip l įvairovė ir t tankis[195].

„L įvairovės metodu išplečiamas k anonimiškumo metodas, siekiant užtikrinti, kad nebebūtų galima rengti determinavimo būdu pagrįstų išpuolių, pasirūpinant, kad kiekvienoje lygiavertiškumo klasėje kiekvienam požymiui būtų priskirta ne mažiau kaip l skirtingų verčių. Vienas

---

[194] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 36-37 psl.
[195] *Ibid*, 19 psl.

iš pagrindinių siektinų tikslų – riboti lygiavertiškumo klasių, kurioms būtų būdingas menkas požymių kintamumas, susidarymą, kad bendrųjų žinių apie tam tikrą duomenų subjektą turinčiam išpuolio vykdytojui visada liktų didelių abejonių dėl savo išvadų. L įvairovės metodas naudingas norint apsaugoti duomenis nuo išpuolių siekiant gauti išvestinių duomenų, kai požymių vertės yra gerai pasiskirsčiusios. Tačiau reikia pabrėžti, kad šiuo metodu negalima panaikinti informacijos nutekinimo galimybės, jeigu požymiai skaidinyje pasiskirstę netolygiai arba priklauso mažam verčių arba reikšminių verčių intervalui. Todėl l įvairovės metodas neapsaugo nuo tikimybinio išvadų darymo išpuolių“[196]. Taigi, pagridininė šio metodo esmė yra ta, kad „kiekvienas lygiavertiškumo klasei priskiriamas požymis turi pasikartoti ne mažiau kaip l kartų, kad išpuolio vykdytojui visada liktų didelių abejonių dėl požymių, net jeigu jis turėtų bendrųjų žinių apie tam tikrą duomenų subjektą“[197]. Siekiant aiškiai parodyti l įvairovės metodo taikymą, C lentelėje pateikiamas pavyzdys kaip originalūs asmens duomenys yra anonimizuojami l įvairovės metodo būdu.

C lentelė. Asmens duomenų anonimizavimo metodas – l įvairovė

	Nonsensitive			Sensitive
	Zip code	Age	Nationality	Condition
1	13053	28	Russian	Heart disease
2	13068	29	American	Heart disease
3	13068	21	Japanese	Viral infection
4	13053	23	American	Viral infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart disease
7	14850	47	American	Viral infection
8	14850	49	American	Viral infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

	Nonsensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	130**	< 30	*	Heart disease
2	130**	< 30	*	Heart disease
3	130**	< 30	*	Viral infection
4	130**	< 30	*	Viral infection
5	1485*	≥ 40	*	Cancer
6	1485*	≥ 40	*	Heart disease
7	1485*	≥ 40	*	Viral infection
8	1485*	≥ 40	*	Viral infection
9	130**	3*	*	Cancer
10	130**	3*	*	Cancer
11	130**	3*	*	Cancer
12	130**	3*	*	Cancer

198

C lentelės kairėje pusėje nurodoma, kad iš duomenų subjektų buvo renkami šie duomenys: pašto kodas (zip code), amžius (age), tautybė (nationality) ir asmens diagnozė (condition). Kaip jau buvo minėta, pagrindinis šio metodo tikslas yra tai, kad „kiekvienas lygiavertiškumo klasei priskiriamas požymis turi pasikartoti ne mažiau kaip l kartų“[199]. Taigi, iš dešinės lentelės pusės galima matyti, kad taikant šį metodą, duomenys buvo lygiaverčiai sugrupuoti į 3 grupes pagal jiems būdingus požymius, pvz. 1 grupė apibendrinta pagal pirmus 3 pašto kodo numerius, panaikindama 2 paskutinius skaičius, kurie yra skirtingi ir gali nurodyti konkretų miestą ar kitą vietovę, taip pat ir

[196] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 19 psl.
[197] *Ibid*, 38 psl.
[198] Johannes Gehrke, Daniel Kifer, Ashwin Machanavajjhala, *„ℓ-Diversity. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security“*, (Springer Boston, 2007). 2 psl.
[199] Europos Komisija, *op.cit.*, 38 psl.

apdorojant amžių, kuris apibendrinus rezultate neviršyja 30 metų, be to buvo visiškai panaikinta informaciją apie tautybę, kurios tikriausiai į vieną grupę nepavyko apibendrinti ir palikta informacija apie asmens diagnozę, kuri tikėtina bus naudojama atitinkamiems tiklams dėl ko buvo atliktas toks anonimizavimas. Panašiu principu buvo apibendrintos 2 ir 3 šios lentelės grupės.

Paskutinis šios grupės aptariamas metodas būtų t tankis. „Ypatingam atvejui, kai požymiai skaidinyje pasiskirstę netolygiai arba kai požymių verčių ar semantinių reikšmių intervalas yra nedidelis, yra skirtas metodas, vadinamas t tankio metodu. Tai patobulintas nuasmeninimo pagal apibendrinimo principą metodas, kurį taikant duomenys sutvarkomi taip, kad būtų sudarytos lygiavertiškumo klasės, kuo labiau atspindinčios pirminį požymių pasiskirstymą pirminiame duomenų rinkinyje“[200]. „T tankio metodas yra patobulintas l įvairovės metodas, nes juo siekiama sudaryti lygiavertiškumo klases, kurioms būtų būdingas panašus į pirminį požymių pasiskirstymas lentelėje. Šis metodas naudingas tada, kai svarbu, kad duomenys būtų kuo panašesni į pirminius; todėl lygiavertiškumo klasei taikomas papildomas apribojimas, pagal kurį kiekvienoje lygiavertiškumo klasėje turėtų būti ne tik mažiau kaip l skirtingų verčių, bet ir kiekviena vertė turi būti pateikta tiek kartų, kiek reikalinga tam, kad būtų atkurtas pirminis kiekvieno požymio pasiskirstymas”[201].

D lentelė. Asmens duomenų anonimizavimo metodas – t tankis.

	Nonsensitive			Sensitive
	Zip code	Age	Nationality	Condition
1	13053	28	Russian	Heart disease
2	13068	29	American	Heart disease
3	13068	21	Japanese	Viral infection
4	13053	23	American	Viral infection
5	14853	50	Indian	Cancer
6	14853	55	Russian	Heart disease
7	14850	47	American	Viral infection
8	14850	49	American	Viral infection
9	13053	31	American	Cancer
10	13053	37	Indian	Cancer
11	13068	36	Japanese	Cancer
12	13068	35	American	Cancer

	Non-Sensitive			Sensitive
	Zip Code	Age	Nationality	Condition
1	1305*	≤ 40	*	Heart Disease
4	1305*	≤ 40	*	Viral Infection
9	1305*	≤ 40	*	Cancer
10	1305*	≤ 40	*	Cancer
5	1485*	> 40	*	Cancer
6	1485*	> 40	*	Heart Disease
7	1485*	> 40	*	Viral Infection
8	1485*	> 40	*	Viral Infection
2	1306*	≤ 40	*	Heart Disease
3	1306*	≤ 40	*	Viral Infection
11	1306*	≤ 40	*	Cancer
12	1306*	≤ 40	*	Cancer

[202]

Kaip jau buvo minėta, t tankio metodu siekiama, kad sudarytos klasės būtų kuo labiau atspindinčios pirminį požymių pasiskirstymą. D lentelės kairėje pusėje yra identiška informacija, kuri buvo pateikta C lentelės kairėje pusėje, tai yra neanonimizuoti duomenų subjektų duomenys. Dešinėje D lentelės pusėje yra duomenys apdoroti t tankio metodu. Kaip jau galima matyti, duomenys palyginus su l įvairovės metodu yra mažiau apdoroti ir turi savyje daugiau informacijos, pvz. pašto

[200] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 39 psl.
[201] *Ibid*, 19 psl.
[202] Johannes Gehrke, Daniel Kifer, Ashwin Machanavajjhala, *„ℓ-Diversity. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security“*, (Springer Boston, 2007), 7 psl.

kodas, kuris šiuo būdu yra mažiau paslėptas, taip pat asmens amžius. Siekiant sugrupuoti tokius duomenys, jie turėjo būti perstatyti (dešinės pusės lentelėje eilės numeris nėra išdėstyti eiliškumo tvarka), kad būtų pasiektas galutinis rezultatas ir kiekvienoje grupėje būtų atitinkamas vienodas rezultatas, kuris palyginus su C lentelės pavyzdžiu, yra išsamesnis.

Taigi į apibendrinimo anonimizavimo metodų grupę įeina šie metodai: agregavimas, k anonimiškumas, l įvairovė bei t tankis. Kiekvienas iš šių metodų pasižymi apibendrinimo principu, bet kiekvieno jų taikymas skiriasi. Agregavimas pasižymi duomenų apibendrinimu siekiant pašalinti perteklinius identifikatorius, tuo tarpu k anonimiškumo metodas užtikrina, kad duomenys bus apibendrinti tokiu būdu, kad iš jų nebus pašalinama informacija ir visi duomenys atsispindės anonimizuotame duomenų rinkinyje. L įvairovės metodas pasižymi duomenų apibendrinamu taip, kad kiekvienas lygiavertiškumo klasei priskiriamas požymis turi pasikartoti ne mažiau kaip l kartų. Ir t tankio anonimizavimo metodas taip pat pasireiškia duomenų apibendrinimu, kuriuo metu sudaromos lygiavertiškumo klasės, kurios atspindi pirminį požymių pasiskirstymą pirminiame duomenų rinkinyje. Pažymėtina, kad ir šiems metodams gali būti būdinga asmens tapatybės nustatymo rizika, ypač tai atvejais, kai aptarti metodai bus taikomi netinkamu būdu.

3.2. Asmens duomenų anonimizavimo metodų privalumai ir trūkumai

Kaip jau buvo ne kartą minėta, asmens duomenų anonimizavimas pasireiškia savo taikomų metodų įvairove. Taip pat buvo išsiaiškinta, kad kiekvieno konkretaus asmens duomenų anonimiziavimo metodo taikymas priklauso nuo tam tikros taikytinos situacijos. Atskleidus kiekvieno metodo ir jų grupės turinį bei principus, vis dar kyla klausimas koks yra kiekvieno metodo patikimumas ir kokiais kriterijais reikėtų vadovaujatis norint juos taikyti praktikoje? Kaip teigia Valstybinė duomenų apsaugos institucija: „žinant pagrindinius kiekvieno metodo privalumus ir trūkumus, lengviau nuspręsti, kaip atitinkamomis aplinkybėmis parengti tinkamą nuasmeninimo procedūrą“[203]. Atsižvelgiant į tai šiame skyriuje bus aptariami asmens duomenų anonimizavimo metodų privalumai ir trūkumai.

Vertinant kiekvieno metodo patikimumą, Europos Komisijos darbo grupė rekomenduoja atsižvelgti į šias 3 rizikas: „1) išskyrimo galimybę, t. y. galimybę išskirti kai kuriuos arba visus įrašus, pagal kuriuos būtų galima nustatyti į duomenų rinkinį įtraukto asmens tapatybę; 2) susiejimo galimybę, t. y. galimybę susieti bent du įrašus, susijusius su tuo pačiu duomenų subjektu

[203] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf, 1 psl.

arba ta pačia duomenų subjektų grupe (toje pačioje duomenų bazėje arba dviejose skirtingose duomenų bazėse). Jeigu išpuolio vykdytojas gali nustatyti (pvz., atlikdamas koreliavimo analizę), kad du įrašai priskirti tai pačiai asmenų grupei, tačiau negali iš tos grupės išskirti pavienių asmenų, tai šiuo metodu apsaugoma nuo išskyrimo, bet neužtikrinama apsauga nuo susiejimo; 3) išvados padarymo galimybę, t. y. galimybę dedukcijos būdu gana tikėtinai nustatyti požymio vertę remiantis kitų požymių rinkinio vertėmis“[204].

Pirmiausia bus aptariami randomizavimo grupės anonimizavimo metodų privalumai bei trūkumai, vėliau ir apibendrinimo grupės metodai.

Vertinant iškraipytų duomenų įterpimo metodą pagal išskyrimo galimybę, Europos Komisija pažymi, kad šiuo atveju šis metodas turi trūkumų, kadangi egzistuoja galimybė išskirti vieno asmens įrašą iš kitų, nors ir neatskleidžiant jo tapatybės, tačiau toks trūkumas gali lemti įrašų mažesnį patikimumą[205]. Taip pat pažymima, kad šiam metodui gali būti būdinga duomenų susiejimo rizika, tačiau įrašų patikimumas bus mažesnis, nes toks įrašas gali būti susietas su dirbtinai įterptu įrašu, kitaip tariant su iškraipytais duomenimis[206]. Vis dėl to EK atkreipia dėmesį, kad „kartais dėl neteisingo jo priskyrimo duomenų subjektui gali kilti didelė ar netgi didesnė rizika, nei tai būtų teisingo priskyrimo atveju“[207]. Vertinant šį metodą iš išvados padarymo galimybės teigiama, kad rizika egzistuoja, tačiau taip pat pažymima, kad yra nedidelė tikimybė, kad išvada bus teisinga[208]. Atsižvelgiant į tai, galima daryti išvadą, kad iškraipytų duomenų metodas turi trūkumų išskyrimo galimybės atžvilgiu, tačiau vertinant šį metodą iš susiejimo bei išvados padarymo galimybių atžvilgiu, šis metodas vis dėl to turi privalumų. Siekiant išvengti minėtų rizikų, Europos Komisija pataria vengti šių klaidų: 1) iškraipymas negali būti pernelyg didelis ir neatitikti duomenų rinkiniui būdingų požymių logikos; ir 2) nevertėtų manyti, kad iškraipytų duomenų įterpimas yra pakankama anonimizavimo priemonė, EK taip pat rekomenduoja prijugti ir kitus anonimizavimo metodus, ypač tuo atveju, kai iškraipytų duomenų kiekis nėra didesnis už duomenų rinkinyje esančios informacijos kiekį[209]. Be to, verta prisiminti, kad 3.1. skyriuje nustant šio metodo turinį, buvo nurodyta, jog šis metodas nebus tiek efektyvus, siekiant išsaugoti kuo daugiau valdytojui naudingos informacijos.

Kitas vertinamas metodas būtų perstatymas. Kaip ir iškraipytų duomenų įterpimo metodas, perstatymas pasireiškia išskyrimo galimybę, t.y. egzistuoja galimybė išskirti su konkrečiu asmeniu susijusius įrašus, tačiau verta pažymėti, kad šiuo atveju toks įrašų patikimumas yra

---

[204] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 12 psl.
[205] *Ibid*, 13 psl.
[206] *Ibid*, 13 psl.
[207] *Ibid*,13 psl.
[208] *Ibid*, 13 psl.
[209] Europos Komisija, *op.cit.*, 13 psl.

mažesnis[210]. „Perstatymas, darydamas įtaką požymiams ir kvaziindikatoriams, gali trukdyti teisingai susieti požymius tame pačiame duomenų rinkinyje ir su kitais duomenų rinkiniais, tačiau vis viena išlieka galimybė atlikti neteisingą susiejimo operaciją, nes tikrasis įrašas gali būti susietas su kitu duomenų subjektu“[211]. Taigi susiejimo rizika šiam metodui taip pat yra būdinga. Tačiau vertinant šį metodą išvados padarymo galimybės prasme, šis metodas turi privalūmų, kadangi „išpuolio vykdytojas, nežinodamas, kurių požymių perstatymas buvo atliktas, turi turėti omenyje, kad toks išvestinių duomenų gavimas yra pagrįstas klaidinga hipoteze, todėl išlieka tik tikimybinė galimybė“[212]. EK atkreipia dėmesį į dažnai pasitaikančias šio metodo taikymo klaidas, t.y. netinkamo požymio pasirinkimą – tuo atveju kai vietoje rizikingų požymių perstatomi nerizikingi, taip pat į atsitiktinį požymių perstatymą, kai tarp dviejų požymių yra stiprus koreliacinis ryšys ir aišku į tai, kad kaip ir iškraipytų įterpimo metodas, perstatymas ne visada bus pakankama anonimizavimo priemonė[213].

Ir paskutinis randomizavimo grupės metodas – diferencinis privatumas pasižymi tokia teigiama savybe kaip negalėjimas išskirti konkretaus asmens įrašų[214]. Tačiau pažymėtina, kad egzistuoja susiejimo ir išvados padarymo galimybės, bet tik tuo atveju, kai yra pasitelkiama daug užklausų[215]. „Norint išvengti susiejimo su bendrosiomis žiniomis, būtina pasistengti pateikti kuo mažiau įrodymų, ar konkretus duomenų subjektas arba jų grupė yra įtraukti į duomenų rinkinį. Duomenų apsaugos požiūriu sunkiausia užduotis – parengti pakankamą iškraipytų duomenų kiekį, pridėtiną prie teisingų atsakymų, kad būtų apsaugotas asmens privatumas kartu nesumažinant teikiamų atsakymų naudingumo”[216]. Europos Komisija taip pat pažymi, kad reikia turėti omenyje, jog šio metodo patikimumas labai priklauso nuo užklausų istorijos saugojimo, t.y. „jeigu nebūtų saugoma užklausų istorija, išpuolio vykdytojas diferencinio privatumo metodu valdomai duomenų bazei galėtų parengti daug užklausų, pagal kurias gaunamos imties dydis būtų nuosekliai mažinamas tol, kol determinavimo būdu arba su gana didele tikimybe išryškėtų vieno duomenų subjekto arba jų grupės konkretus pobūdis“[217].

Kaip matyti randomizavimo grupės metodai turi savo privalumų ir trūkumų, vieni metodai turi daugiau rizikos vertinant duomenų susiejimo galimybės, kiti išvados padarymo galimybės atžvilgiu ir kt. Siekiant nustatyti visų šiame darbe aptartų asmens duomenų anonimizavimo

---

[210] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 14 psl.
[211] *Ibid*, 15 psl.
[212] *Ibid*, 15 psl.
[213] *Ibid*, 15 psl.
[214] *Ibid*, 16 psl.
[215] *Ibid*, 16 psl.
[216] *Ibid*, 16 psl.
[217] *Ibid*, 17 psl.

metodų privalumus ir trūkumus, toliau bus vertinama kita asmens duomenų anonimizavimo grupė – apibendrinimas, o tiksliau jos taikomų metodų patikimumas, remiantis tomis pačiomis Europos Komisijos pasiūlytomis rizikomis. Europos Komisija vertindama apibendrinimo metodų patikimumą, sujungė kelis metodus ir pateikė jų bendrą vertinimą[218].

Pirmiausia vertinami šie metodai: agregavimas ir k anonimiškumas. Nuomonėje dėl nuasmeninimo metodų šie metodai vertinami kaip atsparūs įrašų išskyrimo rizikai, kadangi „turėtų būti nebeįmanoma iš k naudotojų grupės išskirti vieną asmenį“[219]. Vertinant šį metodą susiejimo galimybės atžvilgiu, tikimybė, kad įrašus galima susieti „gali būti gerokai didesnė už tikimybę, kad šie įvesties elementai nesusiejami“[220]. Europos Komisija pažymi, kad pagrindinis šių metodų trūkumas yra tas, kad nėra sudėtinga padaryti teisingą išvadą. „Išties, jeigu visi k asmenų priklauso tai pačiai grupei, tuomet, jeigu žinoma, kuriai grupei asmuo priklauso, nesunku gauti šios savybės vertę“[221]. Kalbant apie dažniausiai pasitaikančias klaidas, EK pažymi, kad siekiant išvengti netinkamo šio metodo taikymo, vertėtų atsižvelgti į apibendrinimo vertes pasirinkimą ir nepasirinkti pernelyg mažos vertes, nes tokiu atveju bus daug didesnė tikimybė teisingai nustatyti asmenį, negu pasirinkus pakankamai plačią vertę[222].

„Kaip ir k anonimiškumo atveju, l įvairovės ir t tankio metodais užtikrinama, kad duomenų bazėje nebūtų galima išskirti su pavieniu asmeniu susijusių įrašų“[223]. Šių metodų savybė yra vertinama kaip privalumas, tačiau duomenų susiejimo atžvilgiu šie metodai pasižymi neigiamai, kadangi išlieka tikimybė, kad bus galima susieti du vienodus įrašus duomenų rinkinyje[224]. Vertinant šiuos metodus iš išvados padarymo rizikos EK pastebi, kad „pagrindinis l įvairovės ir t tankio metodų privalumas k anonimiškumo metodo atžvilgiu yra tas, kad naudojantis duomenų bazėmis, kurioms buvo pritaikyti šie metodai, nebegalima parengti išvestinių duomenų gavimo išpuolių, kurie duotų 100 proc. patikimus rezultatus“.

Kaip matyti iš pateiktų vertinimų kiekvienas metodas turi savo privalumų ir trūkumų. Valstybinė duomenų apsaugos institucija taip pat pažymi, kad „abi nuasmeninimo metodų grupės – duomenų randomizavimas ir apibendrinimas – turi trūkumų, tačiau tam tikromis aplinkybėmis ir

---

[218] Europos Komisija, *„Nuomonė 05/2014 dėl nuasmeninimo metodų“*, 2014. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 17 psl.
[219] *Ibid*, 17 psl.
[220] *Ibid*, 17 psl.
[221] *Ibid*, 17 psl.
[222] *Ibid*, 17 psl.
[223] *Ibid*, 19 psl.
[224] *Ibid*, 19 psl.

sąlygomis kiekviena iš šių grupių gali būti tinkama pageidaujamam tikslui pasiekti priemonė, tuo pačiu nepažeidžiant duomenų subjekto privatumo“[225].

Apibendrinant pateiktą vertinimą pagal Europos Komisijos pasiūlytus rizikos veiksnius (išskyrimo galimybė, susiejimo galimybė, išvados padarymo galimybė), buvo gautos tokios išvados: pakankamai saugūs asmens duomenų anonimizavimo metodai duomenų išskyrimo rizikos atžvilgiu yra agregavimas ir k anonimiškumas, l įvairovė bei diferencinis privatumas (laikantis tam tikrų sąlygų)[226]. Susiejimo galimybės atžvilgiu, pakankamai atsparūs šiai rizikai metodai yra iškaipytų duomenų įterpimas bei diferencinis privatumas, laikantis tam tikrų sąlygų[227]. Ir išvados padarymo rizikos atžvilgiu saugiausi pasirodo praktiškai visi aptarti asmens duomenų anonimizavimo metodai, išskyrus agregavimo ir k anonimiškumo metodų[228]. Atsižvelgiant į gautus rezultatus, autorius daro išvadą, kad iš visų pateiktų asmens duomenų anonimizavimo metodų, labiausiai patikimumą turintis metodas pagal Europos Komisijos pasiūlytus rizikos veiksnius, būtų diferencinis privatumas. Tačiau autorius taip pat nori atkreipti dėmesį, kad tokia išvada nereiškia, kad neverta rinktis kitų asmens duomenų anonimizavimo metodų, nes prisiminus Europos Komisijos rekomendaciją, siekiant užtikrinti visišką asmens duomenų anonimizavimą, pirmiausia reikėtų atsižvelgti į konkrečią situaciją kokį metodą apskritai būtų galima taikyti bei į tai, kad patartina derinti kelis anonimizavimo metodus tarpusavyje, siekiant užtikrinti visišką anonimiškumą.

---

[225] Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf, 3 psl.
[226] Europos Komisija. Nuomonė 05/2014 dėl nuasmeninimo metodų, 2014. Prieiga prie interneto: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf, 25 psl.
[227] *Ibid*, 25 psl.
[228] *Ibid*, 25 psl.

IŠVADOS

1. Asmens duomenų anonimizavimas yra procesas, kuriuo metu pritaikius atitinkamą anonimizavimo metodą visiškai ir negrįžtamai pašalinami tiesioginiai ir netiesioginiai asmens identifikatoriai, ko pasekoje asmens duomenys tampa anoniminiais ir jiems nustoja galioti asmens duomenų apsaugos taisyklės.

2. Asmens duomenų anonimizavimo paskirtis yra trejopa. Pirmiausia, anonimizavimas tai naudos išsaugojimo ir rizikos mažinimo strategija, kuri užtikrina duomenų valdytojui galimybę tvarkyti duomenis atitinkamais tikslais, nesukeliant duomenų apsaugos pažeidimo rizikos. Antra, anonimizavimas užtikrina duomenų subjektams jų duomenų saugumą. Ir trečia, anonimizavimas gali padėti įgyvendinti BDAR įtvirtintą duomenų kiekio mažinimo principą. Taip pat gali būti užtikrinama pusiausvyra, kuri pasireiškia duomenų valdytojo noru pasiekti savo iškeltų tikslų bei duomenų subjekto lūkesčiu, kad jo duomenys būtų tinkamai apsaugoti.

3. Negalėjimas nustatyti asmens tapatybės yra vienas pagrindinių asmens duomenų anonimizavimui taikomų reikalavimų, tačiau kai kuriuose valstybėse jis taikomas skirtingai. Vienur laikomasi griežto reikalavimo dėl negalėjimo asmens identifikuoti jokiais būdais, kitur atsižvelgiama į visas proporcingas pastangas tapatybei nustatyti. Lietuvoje nustatant ar duomenų rinkinys yra tinkamai anonimizuotas ar ne, atsižvelgiama į proporcingas pastangas nustatyti asmens tapatybę, tokias kaip laikas, lėšos ir darbas.

4. Tam tikrais atvejais asmens duomenų anonimizavimas gali būti tapatinamas su tokiomis duomenų saugumo priemonėmis kaip pseudominizavimas, šifravimas ar teismo bylų nuasmeninimas. Tačiau esminiai aspektai, kurie skiria minėtas duomenų saugumo priemones nuo asmens duomenų anonimizavimo yra tai, kad 1) tik asmens duomenų anonimizavimas gali užtikrinti, kad tiesioginiai ir netiesioginiai asmens identifikatoriai bus pašalinti visiškai ir negrįžtamai, tuo tarpu minėtos saugumo priemonės gali užtikrinti tik tai, kad jos bus pašalinamos iš prieinamos erdvės, tačiau pirminė informacija su asmens identifikatoriais bus saugoma pas duomenų valdytoją ar kitą atsakingą asmenį. Ir 2) tik anonimizuotiems duomenims nustoja galioti asmens duomenų apsaugos taisyklės. Pseudominizuoti, šifruoti ir nuasmeninti duomenys vis dar laikomi asmens duomenimis.

5. Asmens duomenų anonimizavimo metodus vertinant pagal šiuos rizikos veiksnius: išskyrimo galimybė, susiejimo galimybė, išvados padarymo galimybė, labiausiai patikimumą turintis asmens duomenų anonimizavimo metodas būtų diferencinis privatumas (identifikatorių pašalinimas pagal užklausas). Tačiau norint pasiekti visišką ir negrįžtamą duomenų anonimizavimą, reikėtų derinti kelis asmens duomenų anonimizavimo metodus tarpusavyje, nes visi šiame darbe nagrinėti metodai (iškraipytų duomenų įterpimas, perstatymas, diferencinis privatumas, agregavimas, k anonimiškumas, l įvairovė ir t tankis) turi tam tikrų trūkumų.

PASIŪLYMAI

1. Peržiūrint bei koreguojant Europos Parlamento ir Tarybos reglamentą (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo siūloma papildyti Reglamento 4 straipsnį, įterpiant šį punktą: 2) *„Asmens duomenų anonimizavimas – visiškas ir negrįžtamas asmens duomenų tiesioginių ir netiesioginių identifikatorių pašalinimas, kuris užtikrina, jog tvarkant tokius duomenis nebus galimybes tiesiogiai arba netiesiogiai nustatyti duomenų subjekto tapatybės“*.

LITERATŪROS SĄRAŠAS

TEISĖS AKTAI.

Lietuvos teisės aktai:

1. „Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas“, *TAR*, 2018;
2. „Lietuvos Respublikos asmens duomenų, tvarkomų nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas, bausmių vykdymo arba nacionalinio saugumo ar gynybos tikslais, teisinės apsaugos įstatymas“, *Valstybės žinios*, 2011;
3. „Lietuvos Respublikos civilinis kodeksas*“, Valstybės žinios*, 2000;
4. „Lietuvos Respublikos Konstitucija“, *Lietuvos Aidas*, 1992;
5. „Teisėjų Tarybos 2015 m. lapkričio 27 d. nutarimas dėl teismų procesinių sprendimų bei teisėjų drausmės bylose priimtų sprendimų viešo skelbimo tvarkos patvirtinimo Nr. 13P- 146-(7.1.2)“, *TAR*, 2015;

Europos Sąjungos teisės aktai:

6. „Europos Parlamento ir Tarybos direktyva (95/46/EB) dėl asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo“, *Europos Sąjungos oficialusis leidinys*, 1995;
7. „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)“. *Europos Sąjungos oficialusis leidinys*, 2016;
8. „Europos Parlamento ir Tarybos reglamentas (ES) 2018/1807 dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“, *Europos Sąjungos leidinys*, 2018.
9. Europos Sąjungos pagrindinių teisių chartija (2016/C 202/02), *Europos Sąjungos oficialus leidinys*, 2016;
10. „Europos žmogaus teisių konvencija“, *Valstybės žinios*, 1995;
11. „Visuotinė žmogaus teisių deklaracija“, *Valstybės žinios,* 2006;

TEISMŲ PRAKTIKA.

Lietuvos:

12. „Klaipėdos apygardos teismo nuosprendis 2019 m. lapkričio 29 d. baudžiamojoje byloje Nr. 1A-185-361/2019“, E-teismai: https://eteismai.lt/byla/189348383075065/1A-185-361/2019?word=teism%C5%B3%20nutartys%20lat;
13. „Lietuvos Aukščiausiojo Teismo nutartis 2008 m. sausio 2 d. civilinėje byloje Nr. 3K-7-2/2008, E-teismai: https://eteismai.lt/byla/275755271714690/3K-7-2/2008;
14. „Lietuvos apeliacinis teismo nutartis 2019 m. lapkričio 29 d. civilinėje byloje Nr. E2-1205-302/2019”, E-teismai: https://eteismai.lt/byla/118204413422338/e2-1205-302/2019?word=teism%C5%B3%20nutartys%20lat;
15. „Lietuvos Vyriausiojo administracinio teismo nutartis 2012 m. liepos 26 d. administracinioje byloje Nr. A-858-2133-12“, Liteko: http://liteko.teismai.lt/viesasprendimupaieska/tekstas.aspx?id=8220958e-b311-4bf4-ba16-980112510ccb;
16. „Lietuvos Vyriausiojo administracinio teismo nutartis 2016 m. gruodžio 12 d. byloje Nr. A-3011-520/2016“, E-teismai, https://eteismai.lt/byla/70939150579211/A-3011-520/2016;
17. „Vilniaus miesto apylinkės teismo nutarimas 2014 m. vasario 26 d. administracinio teisės pažeidimo byloje Nr. A2.11.-1793-295/2014“, E-teismai: https://eteismai.lt/byla/59726336888973/A2_11_-1793-295/2014;

Europos Sąjungos:

18. „Europos Sąjungos Teisingumo teismo sprendimas 2016 m. spalio 19 d. byloje Breyer Nr. C-582/14“. Eur-lex: https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62014CJ0582&from=FR;
19. „Europos Sąjungos Teisingumo Teismo sprendimas 2017 m. gruodžio 20 d. byloje Peter Nowak Nr. C-434/16“, Europos Sąjungos Teisingumo Teismo praktikos apžvalga: https://www.lat.lt/data/public/uploads/2018/03/estt_2017_gruodis.pdf;
20. „Europos Žmogaus Teisių Teismo sprendimas 2009 vasario 10 d. byloje Eerikainen and others v. Finland, peticijos Nr. 3514/02“;
21. „Europos Žmogaus Teisių Teismas sprendimas 1997 m. vasario 25 d. byloje Z. v. Finland, peticijos Nr. 9/1996/627/811, paragrafas 113“;

DOKTRINA.

Lietuvos doktrina:

22. Civilka Mindaugas, Lamanauskas Tomas, Osinaitė G., Sauliūnas Darius, Štitilis Darius, Toliušis S., Ulevičius L., *„Informacinių technologijų teisė“*, Vilnius, 2004;
23. Civilka Mindaugas, Šlapimaitė Lina, *Asmens duomenų samprata elektroninėje erdvėje*. TEISĖ, 2015. Prieiga per internetą: http://www.zurnalai.vu.lt/teise/article/download/8761/7647/;
24. Gruodytė Edita, Milčiuvienė Saulė, *„Anonymization of court decisions in the EU: actual and comparative issues“*, Teisės apžvalga Nr. 2 (18), 2018. Prieiga per internetą: https://www.vdu.lt/cris/bitstream/20.500.12259/60444/1/ISSN2029-4239_2018_N_2_18.PG_60-70.pdf;
25. Meškauskaitė Liudvika, *„Teisė į privatų gyvenimą“*, Vilnius: Registrų centras, 2015;
26. Šindeikis Algimantas, „*Teismų procesinių sprendimų nuasmeninimo konstituncingumo problemos“*, Jurisprudencija, Mykolo romerio universitetas, 2009. Prieiga per internetą: https://www.mruni.eu/upload/iblock/76c/3sindeikis.pdf;
27. Štitilis Darius, Kiškis Mindaugas, Limba Tadas, *„Interneto ir technologijų teisė“*. Vilnius: Registrų centras, 2016;
28. Zaleskis Julius, *„Europos Sąjungos Bendrasis duomenų apsaugos reglamentas ir asmens duomenų apsaugos teisė“*. Vilnius: Registrų centras, 2019;

Užsienio doktrina:

29. Alhajj Reda, Gao Hong, Li Xue, Li Jianzhong, Zaiane Osmar R., „*Advanced Data Mining and Applications“*. Springer, 2017;
30. Antonio Miguel, Ovando Wister, Pancardo Garcia Pablo, Acosta Escalante Francisco Diego, Hernandez Nolasco Jose Adan, „*Intelligent Data Sensing and Processing for Health and Well-being Applications“*, Elsvier, 2018;
31. Balkin Jack M., Eddan Katz, Grimmelmann James, Kozlovski Nimrod, Wagman Shlomit, Zarsky Tal, *„Cybercrime Digital Cops in a Networked Environment“*, New York University Press, 2007;
32. Beyleveld Deryck, Townend David, Rouille-Mirza Segolene, Wright Jessica, *„The Data Protection Directive and Medical Research Across Europe“,* Taylor & Francis, 2017;
33. Calder Alan, *„EU GDPR & EU-US Privacy Shield– A Pocket Guide“*, United Kingdom, 2016;
34. Domingo-Ferrer Josep, Sánchez David, Soria-Comas Jordi*, „Database Anonymization – Privacy Models, Data Utility, and Microaggregation-based Inter-model Connections“.* Morgan & Claypool Publishers, 2016;
35. European Union Agency for Fundamental Rights and Council of Europe, „Handbook on European data protection law“, Luxembourg: Council of Europe, 2018;
36. Gehrke Johannes, Kifer Daniel, Machanavajjhala Ashwin, *„ℓ-Diversity. In: van Tilborg H.C.A., Jajodia S. (eds) Encyclopedia of Cryptography and Security“*, Springer Boston, 2007;

37. Li Kuan-Ching, Jiang Hai, Yang Laurence T., Cuzzocrea Alfredo, „Big Data – Algorithms, Analytics, and Applications“, CRC Press, 2015;
38. Lindon John C., Nicholson Jeremy K., Holmes Elaine, *„The Handbook of Metabolic Phenotyping“*, Elsevier, 2018;
39. Mivule Kato, *„Utilizing noise addition for data privacy, an overview“*, Bowie State University, 2013. Prieiga per internetą: https://arxiv.org/pdf/1309.3958.pdf;
40. Nardelli Enrico, Posadziejewski Sabina, Talamo Maurizio, *„Certification and Security in E-Services– From E-Government to E-Business”*, Springer, 2013;
41. Personal Data protection commission Singapore, *„Guide to basic data anonymisation techniques“*, IAPP, 2018. Prieiga per internetą: https://iapp.org/media/pdf/resource_center/Guide_to_Anonymisation.pdf;
42. Raghunathan Balaji, *„The Complete Book of Data Anonymization – From Planning to Implementation“,* Taylor & Francis Group, LLC, 2013. *http://www.ittoday.info/Excerpts/Data_Anonymization.pdf;*
43. Tamò-Larrieux Aurelia, *„Designing for Privacy and its Legal Framework: Data Protection by Design and Default for the Internet of Things“*, Springer, 2018;
44. Tessier Catherine, Bonnemains Vincent, *„Neuroergonomics“*, Academic Press, 2018;
45. Toom Kristel, Miller Pamela F., *„Research Management“*, Academic Press, 2018. Prieiga per internetą: https://www.sciencedirect.com/topics/biochemistry-genetics-and-molecular-biology/anonymization

KITA:

46. *„Airbnb privatumo politika”.* Žiūrėta 2019 m. spalio 3 d. Preiga per internetą: https://www.airbnb.com/terms/privacy_policy
47. *„Anonymisation and Pseudonymisation of Personal data“*. Žiūrėta 2019 rugsėjo 25 d. Prieiga per internetą:https://www.ucl.ac.uk/data-protection/guidance-staff-students-and-researchers/practical-data-protection-guidance-notices/anonymisation-and#Anonymisation
48. *„Anonymised' data can never be totally anonymous, says study“*. Žiūrėta 2019 spalio 19 d. Prieiga per internetą: https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds;
49. Baltrukėnaitė Jūratė, *„Kokybinių socialinių apklausų anonimizavimo modelis“*. Magistro baigiamasis darbas, Vytauto Didžiojo universitetas, 2019. Prieiga per internetą: https://www.vdu.lt/cris/bitstream/20.500.12259/79175/1/Jurate_Baltrukenaite_md.pdf .

50. *„Data anonymization and GDPR compliance: the case of Taxa 4×35“*. Žiūrėta 2019 spalio 27 d. Prieiga per internetą: https://gdpr.eu/data-anonymization-taxa-4x35/
51. Europos Komisija, *„Apie asmens duomenų apsaugos reformą“*. Žiūrėta 2019 rugsėjo 17 d.. Prieiga per internetą: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_lt;
52. Europos Komisija, *„Nuomone 4/2007 dėl asmens duomenų sąvokos“*, 2007. Prieiga per internetą: https://ec.europa.eu/justice/article-29/documentation/opinion recommendation/files/2007/wp136_lt.pdf;
53. Europos Komisija*, Nuomonė 05/2014 dėl nuasmeninimo metodų*, 2014. Prieiga per internetą: *https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_lt.pdf;*
54. Finnish social science data archive, *„Anonymisation and personal data“*. Žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://www.fsd.uta.fi/aineistonhallinta/en/anonymisation-and-identifiers.html;
55. Gina Kolata, *„Your Data Were 'Anonymized'? These Scientists Can Still Identify You“*, NY times: 2019 liepos 23 d. Prieiga per internetą: https://www.nytimes.com/2019/07/23/health/data-privacy-protection.html;
56. *Google privatumo politika, „Kaip „Google“ anonimizuoja duomenis“*. Žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://policies.google.com/technologies/anonymization?hl=lt;
57. *„Instagram privatumo politika“*. Žiūrėta 2019 spalio 30 d. Prieiga per internetą: https://help.instagram.com/402411646841720
58. *„Yahoo privatumo politika“*. Žiūrėta 2019 m. spalio 30 d. Prieiga per internetą: https://policies.yahoo.com/ie/en/yahoo/privacy/index.htm?redirect=no
59. Kisner Lea, *„Deidentification versus anonymization“*, IAPP, 2019. Prieiga prie interneto: https://iapp.org/news/a/de-identification-vs-anonymization/;
60. Komisijos Komunikatas Europos Parlamentui ir Tarybai, *„Gairės dėl Reglamento dėl laisvo ne asmens duomenų judėjimo Europos Sąjungoje pagrindų“*, 2019 gegužės 29 d. Eur-lex: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=COM:2019:250:FIN;
61. „*Orange privatumo politika“*. Žiūrėta 2019 m. spalio 30 d. Prieiga per internetą: https://www.orange-business.com/sites/default/files/obs-privacy-policy-customers-and-prospects_oct-2019.pdf#chapter8;
62. Pervaiz Zahid, Aref Walid G., Ghafoor Arif, Prabhu Nagabhushana, *„Accuracy-Constrained Privacy-Preserving Access Control Mechanismfor Relational Data“*, Research gate, 2014. Prieiga per internetą: https://www.researchgate.net/publication/261567414_Accuracy-Constrained_Privacy-Preserving_Access_Control_Mechanismfor_Relational_Data;

63. *„Supervision of Taxa 4x35's processing of personal data“*, Datatilsynet, 2019 kovo 18 d. Prieiga per internetą: https://www.datatilsynet.dk/tilsyn-og-afgoerelser/afgoerelser/2019/mar/tilsyn-med-taxa-4x35s-behandling-af-personoplysninger/;
64. Valstybinė duomenų apsaugos inspekcija, *„Ar IP adresas yra asmens duomenys?“*, 2015 gegužės 25 d. ADA: https://www.ada.lt/go.php/lit/1-ar-ip-adresas-yra-asmens-duomenys-2014-m;
65. Valstybinė duomenų apsaugos institucija, *„Nuasmeninimo metodai“,* 2015. Prieiga per internetą: https://vdai.lrv.lt/uploads/vdai/documents/files/Rekomend_nuasmeninimo_metodai_2015.pdf;
66. Vikipedija, *„Google*“. Žiūrėta 2019 lapkričio 3 d. Prieiga per internetą: https://lt.wikipedia.org/wiki/Google;
67. Vikipedija, *„Instagram*“. Žiūrėta 2019 spalio 30 d. Prieiga per internetą: https://lt.wikipedia.org/wiki/Instagram.

ANOTACIJA LIETUVIŲ IR ANGLŲ KALBOMIS

Magistro baigiamajame darbe nagrinėjamas viena iš asmens duomenų saugumo priemonių – asmens duomenų anonimizavimas. Siekiama ištirti asmens duomenų anonimizavimo sampratą bei galimybę užtikrinti duomenų apsauga pasitelkiant anonimizavimu. Atsižvelgiant į tai nustatomi pagrindiniai asmens duomenų anonimizavimo aspektai, tokie kaip anonimizavimo samprata, jo paskirtis ir pagrindiniai taikomi reikalavimai, taip pat asmens duomenų ir anoniminių duomenų sampratos. Siekiant paneigti klaidingą tapatinimą su pseudominizavimu, duomenų šifravimu ir teismo bylų nuasmeninimu yra atribojamos šios duomenų saugumo priemonės nuo asmens duomenų anonimizavimo. Taip pat tiriami asmens duomenų anonimizavimo metodai ir lyginami tarpusavyje.

Nustatyta, kad asmens duomenų anonimizavimas pasireiškia visišku ir negrįžtamu asmens identifikatorių pašalinimu, ko pasekoje duomenys tampa anoniminiais ir jiems nustoja galioti asmens duomenų apsaugos principai ir kiti reikalavimai. Be to, asmens duomenų anonimizavimas negali būti tapatinamas su kitomis duomenų saugumo priemonėmis, nes jie negali užtikrinti duomenų subjekto anonimiškumo, o anonimizavimas gali. Taip pat išsiaiškinta, kad asmens duomenų anonimizavimo metodai visi turi tam tikrų trūkumų, todėl norint pasiekti visišką anonimizavimą reikia derinti kelis anonimizavimo metodus tarpusavyje.

Reikšminiai žodžiai: anonimizavimas, asmens duomenys, anonimiškumas, duomenų apsauga, duomenų saugumo priemonės.

One of the security measures of personal data – Personal data anonymization – is analyzed in this master's thesis. The aim is to explore the concept of anonymization of personal data and the possibility of ensuring data protection through anonymization. In this context, the main aspects of anonymization of personal data, such as the concept of anonymization, its purpose and basic requirements, as well as the concepts of personal data and anonymized data, are identified. These data security measures are separated from the anonymization of personal data in order to counteract misidentification with pseudominization, data encryption and anonymisation of court cases. Methods of anonymisation of personal data are also investigated and compared with each other.

It has been established that the anonymization of personal data results in the complete and irreversible removal of personal identifiers, as a result of which the data becomes anonymous and the personal data protection principles and other requirements cease to apply. In addition, the anonymization of personal data cannot be assimilated to other data security measures because they

cannot guarantee the anonymity of the data subject, and anonymization can. It has also been found that personal data anonymization methods all have certain drawbacks, so it is advisable to combine several anonymization methods with each other to achieve complete anonymization.

Keywords: anonymization, personal data, anonymity, data protection, data security measures.

SANTRAUKA LIETUVIŲ KALBA

Zorina Julija (2019). *Asmens duomenų anonimizavimas* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas.

Asmens duomenų anonimizavimas Lietuvoje nėra tiesiogiai įtvirtintas kaip tinkama duomenų saugumo priemonė, todėl ši priemonė šiai dienai nėra taip plačiai žinoma bei taikoma praktikoje kaip antai pseudominizavimas arba šifravimas, kurie yra tiesiogiai įtvirtinti Bendrajame duomenų apsaugos reglamente. Atsižvelgiant į tai magistro baigiamojo darbo tyrimo tikslas – ištirti asmens duomenų anonimizavimo sampratą bei galimybę užtikrinti duomenų apsauga pasitelkiant anonimizavimu. Šiam tikslui pasiekti iškelti šie uždaviniai: ištirti asmens duomenų anonimizavimo sampratą, taip pat atskleisti jos paskirtį ir pagrindinius reikalavimus; atriboti asmens duomenų anonimizavimą nuo kitų duomenų saugumo priemonių, tokių kaip pseudominizavimas, šifravimas ir teismo bylų nuasmeninimas; ištirti pagrindinius asmens duomenų anonimizavimo metodus, nustatyti kiekvieno jų turinį ir įvertinti jų privalumus bei trūkumus.

Mokslinį darbą sudaro: įvadas, trys dėstomosios dalys, išvados, pasiūlymai. Pirmoje dėstomojoje dalyje nustatomi pagrindiniai asmens duomenų anonimizavimo aspektai, tokie kaip anonimizavimo samprata, jo paskirtis ir pagrindiniai taikomi reikalavimai, taip pat asmens duomenų ir anoniminių duomenų sampratos. Taip pat šioje dalyje nagrinėjamas asmens duomenų ir anoniminių duomenų teisinis ryšys, šių sampratų teisinio reglamentavimo skirtumai ir jų vaidmuo asmens duomenų anonimizavimo procese. Antroje mokslinio darbo dalyje siekiama nustatyti kitų duomenų saugumo priemonių sampratą, plačiai išnagrinėti tokias priemones kaip pseudominizavimas, šifravimas ir teismo bylų nuasmeninimas, siekiant atriboti minėtas duomenų saugumo priemones nuo asmens duomenų anonimizavimo. Trečioje šio darbo dalyje nagrinėjami asmens duomenų anonimizavimo metodai, ištiriamas ir plačiai atskleidžiamas kiekvienas metodas, jo taikymo galimybės, taip pat vertinami kiekvieno metodo privalumai bei trūkumai.

Atlikus tyrimą buvo nustatyta, kad asmens duomenų anonimizavimas yra procesas, kuriuo metu visiškai ir negrįžtamai pašalinami tiesioginiai ir netiesioginiai asmens identifikatoriai, ko pasekoje asmens duomenys tampa anoniminiais ir jiems nustoja galioti asmens duomenų apsaugos taisyklės. Taip pat buvo nustatyta, kad asmens duomenų anonimizavimo pasireiškia trejopai: 1) užtikrina duomenų valdytojui galimybę tvarkyti duomenis atitinkamais tikslais, nesukeliant duomenų apsaugos pažeidimo rizikos; 2) užtikrina duomenų subjektams jų duomenų saugumą; ir 3) anonimizavimas gali padėti įgyvendinti duomenų kiekio mažinimo principą. Buvo prieita išvados, jog kai kurios valstybės laikosi griežto požiūrio dėl negalėjimo asmens identifikuoti jokiais būdais,

kitos teigia, jog reikia atsižvelgti į proporcingas pastangas tapatybę nustatyti. Taip pat buvo nustatyti esminiai aspektai, kurie skiria minėtas duomenų saugumo priemones nuo asmens duomenų anonimizavimo: 1) tik asmens duomenų anonimizavimas gali užtikrina, kad tiesioginiai ir netiesioginiai asmens identifikatoriai bus pašalinti visiškai ir negrįžtamai, tuo tarpu minėtos saugumo priemonės gali užtikrinti tik tai, kad jos bus pašalinamos iš prieinamos erdvės, tačiau pirminė informacija su asmens identifikatoriais bus saugoma pas duomenų valdytoją ar kitą atsakingą asmenį. Ir 2) tik anonimizuotiems duomenims nustoja galioti asmens duomenų apsaugos taisyklės. Pseudominizuoti, šifruoti ir nuasmeninti duomenys vis dar laikomi asmens duomenimis. Taip pat atlikus asmens duomenų anonimizavimo metodų vertinimą pagal šiuos rizikos veiksnius: išskyrimo galimybė, susiejimo galimybė, išvados padarymo galimybė, labiausiai patikimumą turintis asmens duomenų anonimizavimo metodas būtų diferencinis privatumas (identifikatorių pašalinimas pagal užklausas), tačiau visišką duomenų anonimizavimą galima pasiekti derinant kelis anonimizavimo metodus tarpusavyje.

SUMMARY IN ENGLISH

Zorina Julija (2019). Personal data anonymization (Master‘s thesis). Vilnius: Mykolas Romeris University.

The personal data anonymization is not directly enshrined in Lithuania as an appropriate means of data security, so this tool is not as widely known and applied in practice today as pseudominization or encryption, which are directly enshrined in the General Data Protection Regulation. With this in mind, the purpose of this Master's thesis is to investigate the concept of personal anonymization and the possibility of ensuring data protection through anonymization. To achieve this goal the following tasks have been set: to explore the concepts of anonymization of personal data and its components, as well as to reveal its purpose and basic requirements; to distinguish between the anonymization of personal data and other data security measures, such as pseudominization, encryption and the anonymisation of court cases; to investigate the main methods of anonymization of personal data, to determine their content and to evaluate their advantages and disadvantages.

Master's thesis consists of introduction, three parts, conclusions and suggestions. The first section sets out the key aspects of anonymization of personal data, such as the concept of anonymization, its purpose and basic requirements, as well as the concepts of personal data and anonymous data. This section also examines the legal relationship between personal data and anonymous data, the differences in the legal regulation of these concepts, and their role in the process of anonymization of personal data. The second part of the thesis aims to establish the notion of other data security measures, and extensively examine tools such as pseudominization, encryption and the anonymisation of court cases to distinguish the above data security measures from the anonymization of personal data. The third part of this paper examines methods of personal data anonymization, explores and extensively discloses each method, its application capabilities, and assesses the advantages and disadvantages of each method.

The investigation revealed that the anonymization of personal data is the process of completely and irrevocably removing direct and indirect personal identifiers, resulting in personal data becoming anonymous and ending personal data protection rules. It has also been established that the anonymization of personal data occurs in three ways: (1) it enables the controller to process the data for the relevant purposes without risking a breach of data protection; 2) ensure the security of the data of the data subjects; and (3) anonymization can contribute to the data minimization principle. It has been concluded that some states take a strict approach regarding the inability to identify a

person by any means, while others argue that proportionate efforts to identify should be taken into account. Essential aspects have also been identified that differentiate the aforementioned data security measures from the anonymization of personal data: (1) only the anonymization of personal data can ensure that direct and indirect personal identifiers are completely and irreversibly removed, whereas the said security measures can only ensure that they will be removed from the accessible space, but primary information with personal identifiers will be stored with the controller or other responsible person. And (2) only anonymized data will cease to be covered by personal data protection rules. Pseudominized, encrypted and anonymised data are still considered personal data. Also, the evaluation of personal data anonymization methods against the following risk factors: isolation, linking, deduction, the most reliable method of anonymizing personal data would be differential privacy (query identifiers removal), but complete anonymization of data can be achieved by combining several anonymization methods between.

PATVIRTINIMAS APIE ATLIKTO DARBO SĄŽININGUMĄ

PATVIRTINIMAS APIE ATLIKTO DARBO SĄŽININGUMĄ

2019-11-24

Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),
Mykolo Romerio teisės mokyklos, civilinės ir verslo teisės programos
(fakulteto / instituto, programos pavadinimas)

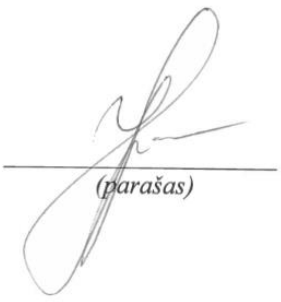
Studentas (-ė) ____ Julija Zorina _____,
(vardas, pavardė)

patvirtinu, kad šis magistro baigiamasis darbas

„Asmens duomenų anonimizavimas“:

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

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



_____ _____Julija Zorina_____
(parašas) *(vardas, pavardė)*