ISSN 2029–7564 (online)
SOCIALINĖS TECHNOLOGIJOS
SOCIAL TECHNOLOGIES
2011, 1(1), p. 61–80.

TEISINĖ APLINKA SIEKIANT IŠVENGTI TAPATYBĖS VAGYSTĖS ELEKTRONINĖJE ERDVĖJE: JAV IR LIETUVOS TEISĖS AKTŲ LYGINAMOJI ANALIZĖ

Darius Štitilis
Paulius Pakutinskas
Inga Dauparaitė
Marius Laurinaitis

Mykolo Romerio universitetas, Lietuva, stitilis@mruni.eu

Abstraktas

Temos aktualumas. Sparčiai auganti interneto ekonomika turi ir neigiamų padarinių. Vienas iš jų – tapatybės vagystė elektroninėje erdvėje. Dėl tapatybės vagystės elektroninėje erdvėje daroma žala paprastiems vartotojams, finansų institucijoms ir galiausiai visai ekonomikai[1]. Be to, tapatybės vagystė elektroninėje erdvėje tapo viena iš pelningiausių nusikalstamų veikų[2].

Asmens tapatybės vagystė elektroninėje erdvėje santykinai nauja pavojinga ir žalinga asmeniui bei visuomenei veika. Dėl šios priežasties pastaruoju metu mokslinėse diskusijos keliamas tapatybės vagystės elektroninėje erdvėje tinkamo teisinio reguliavimo klausimas. Atsižvelgiant į problemos santykinį naujumą nacionaliniai įstatymai skirtingai reglamentuoja šią veiką, todėl labai svarbu įvertinti esamą patirtį ir išanalizuoti tapatybės vagystės elektroninėje erdvėje teisinį reglamentavimą.

1 Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50:240.

2 Higgins, E. G. Cybercrime: An Introduction to an Emerging Phenomen. McGraw-Hill, 2010, p. 67.

ISSN 2029-7564 (online)
https://www.mruni.eu/lt/mokslo_darbai/st/apie_leidini/
https://www.mruni.eu/en/mokslo_darbai/st/apie_leidini/index.php

Viena iš lyderiaujančių valstybių teisiškai reglamentuojant tapatybės vagystę elektroninėje erdvėje – JAV (šioje valstybėje taip pat didelis tokių pavojingų veikų skaičius). Todėl šiame straipsnyje teisinė aplinka analizuojama lyginant dviejų valstybių – JAV ir Lietuvos – teisės aktus, susijusius su tapatybės vagyste elektroninėje erdvėje. Lyginamos šios teisinio reguliavimo sritys, nuo kurių, autorių nuomone, priklauso sėkminga kova su tapatybės vagyste elektroninėje erdvėje: asmens duomenų apsauga, elektroninių duomenų saugumas, tapatybės nustatymas, baudžiamoji atsakomybė bei specialūs teisės aktai dėl tapatybės vagystės elektroninėje erdvėje.

Mokslinių tyrimų tikslas – lyginamuoju metodu išanalizuoti JAV ir Lietuvos teisės aktus, susijusius su tapatybės vagyste elektroninėje erdvėje.

Tyrimo objektas – tapatybės vagystė elektroninėje erdvėje, jos teisinis reglamentavimas.

Metodologija**. P**agrindinis tyrimas atliekamas lyginamuoju metodu (siekiama nustatyti tiriamo objekto, t. y. JAV ir Lietuvos teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje, panašumus ir skirtumus), be to, taikomi loginis, sisteminis, analizės, statistinis ir kiti tyrimo metodai.

Analizuojamos problemos ištirtumas. Mokslinėje literatūroje analizuojama tapatybės vagystė elektroninėje erdvėje. Tiriami socialiniai, teisiniai ir kiti šios pavojingos veikos aspektai. Taip pat, aptariami atskirų valstybių (daugiausia JAV) teisinio reguliavimo dokumentai. Pastaruoju metu aktyviai mokslinę veiklą minėtoje srityje vykdo nemažai mokslininlų (S. W. Brenner, S. Ghosh, E. Turrini, G. E. Higgins, J. T Wells ir kt.). Tačiau iki šiol teisinė aplinka, susijusi su tapatybės vagyste elektroninėje erdvėje, lyginamuoju aspektu (JAV ir Lietuvoje) nebuvo analizuota.

Rezultatai. Atlikus tyrimą nustatyti JAV ir Lietuvos teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje, panašumai ir trūkumai, išdėstytos prielaidos dėl JAV gerosios praktikos, reglamentuojant tapatybės vagystę elektroninėje erdvėje, taip pat įžvalgos dėl atitinkamo teisinio reguliavimo trūkumų.

Praktinė reikšmė. Tyrimo rezultatai naudingi Lietuvoje tobulinant su tapatybės vagyste elektroninėje erdvėje susijusį teisinį reguliavimą.

Orginalumas/Vertingumas. Mokslinėje literatūroje tapatybės vagystė elektroninėje erdvėje pristatoma kaip socialinis-teisinis reiškinys, nagrinėjami teisės aktai, susiję su šiuo reiškiniu, tačiau iki šiol nebuvo atlikta JAV (kaip vienos iš lyderiaujančių valstybių reglamentuojant tapatybės vagystę elektroninėje erdvėje) ir Lietuvos lyginamosios teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje, analizės. Tyrimas vertingas tuo, jog lyginamosios analizės būdu lyginamos kelios teisinio reguliaivmo sritys, susijusios su tapatybės vagyste elektroninėje erdvėje, ir tokiu būdu atskleidžiami atitinkamo teisinio reguliavimo skirtumai. Daromos prielaidos dėl gerosios teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, praktikos.

Raktažodžiai: tapatybės vagystės elektroninėje erdvėje teisinė aplinka.

Tyrimo tipas: tyrimo pristatymas (lyginamoji teisės aktų analizė).

1. Asmens duomenų apsaugos teisinis reguliavimas

Pažymėtina, kad asmens duomenų apsaugos teisiniam reguliavimui Lietuvoje daro įtaką tarptautinis ir regioninis teisinis reguliavimas. Tarptautiniu mastu galioja 1981 m. Strasbūro konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu[3] (toliau – Strasbūro konvencija, Konvencija), prie kurios šalys jungiasi savarankiškai ir savanoriškai. Europos Sąjungos lygiu asmens duomenų teisinės apsaugos reguliavimas remiasi 1995 m. spalio 24 d. Europos Parlamento ir Tarybos direktyva Nr. 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo[4] (toliau – Direktyva). Tai yra du pagrindiniai privalomojo pobūdžio teisės aktai, reglamentuojantys asmens duomenų apsaugą tarptautiniu ir Europos Sąjungos (regioniniu) lygiu, todėl per šių dviejų teisės aktų prizmę bus lyginamas asmens duomenų teisinis reguliavimas Lietuvoje ir JAV.

Lietuvoje, kaip ir kiekvienoje Europos Sąjungos valstybėje narėje, Direktyvą įgyvendina Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas[5], kurio tikslas – ginti žmogaus privataus gyvenimo neliečiamumo teisę tvarkant asmens duomenis. Be to, Lietuva 2000 m. vasario 11 d. pasirašė, o 2001 m. birželio 1 d. ratifikavo Strasbūro konvenciją, kuri Lietuvoje įsigaliojo nuo 2001 m. spalio 1 d. Tuo tarpu JAV nėra prisijungusi prie 1981 m. Strasbūro konvencijos[6] ir asmens duomenų apsaugos reguliavimui šioje valstybėje jokios regioninės ar tarptautinės iniciatyvos nedaro įtakos.

Lietuva priklauso europietiškajam asmens duomenų apsaugos reguliavimo modeliui, kurio esmė yra visapusiškas teisinis reguliavimas: asmens duomenų apsaugos sritį reglamentuoja vienas bendras – Lietuvos Respublikos asmens duomenų teisinės apsaugos – įstatymas, įtvirtinantis pagrindinius teisėto asmens duomenų tvarkymo reikalavimus, duomenų subjekto teises; reglamentuojantis duomenų saugumo ir duomenų teikimo klausimus; nustatantis instituciją, atsakingą už asmens duomenų apsaugą, užtikrinantis asmens duomenų valdytojų registracijos minėtos institucijos duomenų bazėje privalomumą; nustatantis reikalavimą gauti išankstinį leidimą norint tvarkyti asmens duomenis; numatantis skundų nagrinėjimo ir tyrimo tvarką bei atsakomybę už įstatymo nuostatų pažeidimus.

Nepaisant JAV ir Europos Sąjungos bendro siekio užtikrinti asmenų teisę į privatumą, JAV požiūris į privatumą yra kitoks nei Europos Sąjungoje[7]. JAV asmens duomenų apsaugos reguliavimas pasižymi sektorinių įstatymų ir savireguliacinio modelių bruo-

---

3 Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. *Valstybės žinios*. 2001, Nr. 32-1059.

4 Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus]. [1995] OL L281/31 [žiūrėta 2011-05-03]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF>.

5 Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios.* 1996, Nr. 63-1479; 2003, Nr. 15-597; 2008, Nr. 22-804.

6 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (entered into force on 1 October 1985) [interaktyvus]. CETS 108 [žiūrėta 2011-05-03]. <http**:**//conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=26/04/2011&CL=ENG>.

7 Kuner, C. European Data Privacy law and Online Business. *Oxford: Oxford University Press*, 2003, p. 279.

žais: skirtingais įstatymais reguliuojamos atskiros asmens duomenų apsaugos sritys, pavyzdžiui, asmens duomenų tvarkymas telekomunikacijų sektoriuje, taip pat taikomi tam tikri elgesio kodeksai asmens duomenų apsaugos srityje. Dėl tokio asmens duomenų apsaugos reguliavimo JAV susiduriama su tokiomis problemomis, kaip pakankamai silpna asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą, taikymas ir problematiškas jų įgyvendinimas.

Taigi JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Lietuvos asmens duomenų reguliavimo modelio, nors abi valstybės turi bendrą tikslą – stiprinti savo piliečių privatumo apsaugą. JAV yra taikomi kitokie duomenų tvarkymo apsaugos standartai. Jie daugeliu požiūrių yra ne tokie griežti kaip Lietuvoje ir apskritai Europos Sąjungoje. Valstijos per bendrąją teisę ir įstatymus sukūrė skirtingus asmeninės informacijos apsaugos lygius. Panašiai federaliniu lygmeniu JAV privatumo apsauga plėtojosi sektorius po sektoriaus, kuriant daugybę įstatymų, numatančių skirtingus asmens duomenų apsaugos standartus, priklausomai nuo asmeninės informacijos rūšies ir pobūdžio, kai kurią informaciją, netgi labai jautrią, paliekant visai be jokios įstatymo apsaugos[8].

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas įtvirtina pagrindinius asmens duomenų apsaugos principus, tokius kaip: tikslo nustatymo, teisėtumo, asmens duomenų kokybės, proporcingumo, saugumo užtikrinimo, panaudojimo apribojimo, draudimo tvarkyti ypatingus asmens duomenis, individualaus dalyvavimo (duomenų subjekto teisių), atvirumo, priežiūros ir sankcijų. Be to, įstatymas įtvirtina, kad asmens duomenys teikiami duomenų gavėjams trečiosiose valstybėse, jeigu šiose valstybėse yra tinkamas asmens duomenų teisinės apsaugos lygis[9]. Būtent dėl paskutinio reikalavimo JAV, siekiant nutiesti tiltą tarp skirtingų požiūrių į asmens duomenų apsaugą, Prekybos departamentas, pasitaręs su Europos Komisija, sukūrė „saugaus uosto“ sistemą (Europoje patvirtinta 2000 m.), kurios pagrindas yra septyni „saugaus uosto“ principai[10]: pranešimo, pasirinkimo, perdavimo tretiesiems asmenims, prieigos, saugumo, duomenų vientisumo ir įgyvendinimo.

Pažymėtina, kad Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme įtvirtinti teisėto asmens duomenų tvarkymo principai yra imperatyvaus pobūdžio, tuo tarpu JAV „saugaus uosto“ programa, priešingai, – remiasi savanoriškumo principu: organizacijos, kurios nori tapti šios programos narėmis, turi užsiregistruoti; be to, jos turi atitikti daugelį standartų, kurie yra nustatyti jų atitikimo Direktyvos 25 straipsnyje numatytam reikalavimui įvertinti.

---

8 Civilka, M. Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste [interaktyvus]. p. 29 [žiūrėta 2011-05-03]. <http://www.google.lt/url?q=http://ututi.lt/subject/VU/EF/elektroninis_verslas/file/3412/get&sa=U&ei=CIrBTYTr GcqYOsXO7Z0I&ved=0CAsQFjAA&usg=AFQjCNGhewAzJu8FWWwu2xDHpalcdnv-sg>.

9 Asmens duomenų teisinės apsaugos lygis vertinamas atsižvelgiant į visas aplinkybes, susijusias su duomenų teikimu, ypač į trečiojoje valstybėje, į kurią ketinami teikti asmens duomenys, galiojančius įstatymus, kitus teisės aktus bei duomenų valdytojo parengtus dokumentus, užtikrinančius asmens duomenų teisinę apsaugą, į teikiamų duomenų pobūdį, duomenų tvarkymo būdus, tikslus, trukmę, saugumo priemones, kurių bus laikomasi toje valstybėje.

10 „Saugaus uosto“ principai [interaktyvus]. [žiūrėta 2011-05-03]. <https://www.export.gov/safeharbor/eu/eg_main_018476.asp>.

„Saugaus uosto“ sistema yra svarbi tuo, kad JAV organizacija, kuri yra „saugaus uosto“ narė, garantuoja „pakankamą“ privatumo apsaugą, kaip tai apibrėžia Direktyva. Vis dėlto JAV yra taikomi kitokie asmens duomenų apsaugos standartai, kurie daugeliu požiūrių yra žemesni nei Lietuvoje. Be to, laikoma, kad JAV numatyti principai negali pakeisti nacionalinio teisinio reguliavimo asmens duomenų teisinės apsaugos srityje[11].

Vis dėlto, nepaisant tam tikrų asmens duomenų teisinės apsaugos trūkumų, ES yra pripažinusi, kad, su tam tikromis išlygomis ir taikant tam tikras sąlygas, JAV „saugaus uosto“ principai gali užtikrinti tinkamą asmens duomenų apsaugos lygį[12].

Už Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, išskyrus 8 straipsnį, vykdymo priežiūrą ir kontrolę atsakinga Valstybinė duomenų apsaugos inspekcija, kurios svarbiausi veiklos tikslai yra plėtoti duomenų apsaugą, prižiūrėti asmens duomenų valdytojų veiklą tvarkant asmens duomenis, kontroliuoti asmens duomenų tvarkymo teisėtumą, kovoti su duomenų tvarkymo pažeidimais ir užtikrinti duomenų subjekto teisių apsaugą[13]. JAV pagrindinės institucijos, atsakingos už „saugaus uosto“ principų laikymąsi, yra Federalinė prekybos komisija, Transporto departamentas ir Prekybos departamentas. Pavyzdžiui, JAV Federalinė prekybos komisija gali pareikalauti laikytis administracinių nurodymų ir skirti baudą iki 12 000 dolerių už kiekvieną pažeidimo dieną. Jei organizacija nuolat pažeidžia „saugaus uosto“ reikalavimus ir dėl to pradedama abejoti jos patikimumu, organizacija privalo apie tai pranešti Prekybos departamentui. Už nepranešimą numatyta baudžiamoji atsakomybė[14].

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo 53 straipsnis įtvirtina banketinę teisės normą, kad asmenims, pažeidusiems šį įstatymą, taikoma įstatymų nustatyta atsakomybė. Pavyzdžiui, Administracinių teisės pažeidimų kodekso[15] $214^{(16)}$ straipsnis numato atsakomybę už duomenų subjekto teisių pažeidimą, $214^{(17)}$ straipsnis – už Valstybinės duomenų inspekcijos pareigūnų teisėtų nurodymų nevykdymą, $214^{(14)}$ straipsnis – už neteisėtą asmens duomenų tvarkymą, $214^{(23)}$ straipsnis – už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje. Sankcijos už šiuos pažeidimus yra labai nedidelės, iki 2 000 litų. Taigi, Lietuvoje už asmens duomenų teisinės apsaugos reikalavimų pažeidimą iš esmės taikoma administracinė atsakomybė, tačiau sankcijos už pažeidimus keletą kartų mažesnės nei JAV.

Atlikus JAV ir Lietuvos asmens duomenų apsaugos teisinio reguliavimo analizę, galima daryti išvadą, kad JAV asmens duomenų apsaugos teisinė sistema labai skiriasi nuo Lietuvos: JAV požiūris į asmens duomenų apsaugą yra paremtas sektoriniu reguliavimu ir savireguliacija, tuo tarpu Lietuvoje – visapusišku teisiniu reguliavimu. JAV

11 Kuner, C. European Data Privacy law and Online Business. *Oxford: Oxford University Press*, 2003, p. 279.

12 Komisijos 2000 m. liepos 26 d. sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto“ privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV Komercijos departamento pateiktų „Dažnai užduodamų klausimų”. [2000] OL L 215, preambulės 5 p.

13 Valstybinė duomenų apsaugos inspekcija [interaktyvus]. Vilnius [žiūrėta 2011-05-03]. < http://www.ada.lt>.

14 False Statements Act (18 U.S.C. § 1001) [interaktyvus]. [žiūrėta 2011-05-03]. <http://www.law.cornell.edu/uscode/18/usc_sec_18_00001001----000-.html>.

15 Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1.

nėra vieno bendro pagrindinio asmens duomenų apsaugą reglamentuojančio įstatymo, o duomenų tvarkymo atžvilgiu vadovaujamasi „saugaus uosto“ sistema ir yra taikomi kitokie apsaugos standartai, kurie daugeliu požiūrių yra žemesni nei Lietuvoje. JAV, priešingai nei Lietuvoje, gana silpnai reglamentuota asmens duomenų apsauga, ribotas įstatymų, reglamentuojančių asmens duomenų apsaugą, taikymas ir problemiškas jų įgyvendinimas, ir nepaisant to, jog, Europos Sąjungos nuomone, JAV užtikrina tinkamą asmens duomenų apsaugą, visos paminėtos problemos sudaro prielaidas elektroninėje erdvėje įvykdyti tapatybės vagystę ir už šią veiką išvengti atsakomybės. Tačiau reikėtų atkreipti dėmesį į sankcijas už asmens duomenų apsaugos pažeidimus, kurios JAV kaletą kartų didesnės nei Lietuvoje ir turėtų labiau atgrasinti potencialius pažeidėjus nuo galimų pažeidimų.

2. Teisinė aplinka elektroninės informacijos saugos srityje

Pastaruoju metu visame pasaulyje elektroninės informacijos saugai skiriama vis daugiau dėmesio tiek techniniu, tiek ir teisiniu požiūriu. Informacijos sauga (saugumas) suprantamas kaip informacijos bei sistemos infrastruktūros apsauga nuo atsitiktinio ar tyčinio, natūralaus ar dirbtinio pobūdžio poveikio, galinčio sukelti žalą informacijos ar sistemos infrastruktūros savininkams bei vartotojams.

Elektroninės informacijos saugos aplinkos klausimus būtų galima suskirstyti į keturias pagrindines grupes: normatyvinę (įstatymai, įstatymų įgyvendinamieji aktai, standartai ir kt.), administracinę (organizacijos vadovybės vykdomi bendro pobūdžio veiksmai), procedūrinę (konkretūs su konkrečiais asmenimis susiję saugumo veiksmai), programinę techninę (vykdomi konkretūs techninio pobūdžio veiksmai)[16].

Atsižvelgiant į šio straipsnio tikslą plačiau šiame skyriuje bus nagrinėjami būtent pirmosios – normatyvinės – elektroninės informacijos saugos aplinkos klausimai Lietuvoje ir JAV.

Vienas iš pagrindinių teisės aktų JAV, reguliuojančių informacijos saugos sritį, – Federalinis informacijos saugos valdymo įstatymas[17], kuris buvo priimtas 2002 m., kaip E. valdžios įstatymo dalis, ir kuriame pabrėžiama informacijos saugos svarba ekonomikai ir nacionaliniam saugumui JAV. Tuo tarpu Lietuva elektroninės informacijos saugos reguliavimo prasme neturi tokių senų tradicijų kaip Europos valstybės[18]. Lietuvoje nėra įstatymo, kuris būtų skirtas tik informacijos saugai reguliuti, o elektroninės informacijos saugos klausimus reglamentuoja daugybė įstatymų ir poįstatyminių aktų[19]. Pavyzdžiui,

16 Kiškis, M., *et al. Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006, p. 38–39.

17 Federal Information Security Management Act, 2002 // US code, Title 44, Chapter 35, Subchapter III [interaktyvus]. [žiūrėta 2011-05-03]. < http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35_20_III.html >.

18 Štitilis, D.; Paškauskas, Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*. 2007, 92 (2): 38.

19 Holistinio teisinio elektroninės informacijos saugos reguliavimo apraiška galima vadinti Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo projektą (buvo parengtas 2007 m.), tačiau šis projektas nebuvo priimtas.

teisės normos, reglamentuojančios elektroninės informacijos saugą, įtvirtintos Lietuvos Respublikos asmens duomenų teisinės apsaugos (30 straipsnis), Elektroninių ryšių (62 straipsnis), Elektroninio parašo ir Valstybės registrų įstatymuose (20 straipsnis), taip pat daugelyje poįstatyminių teisės aktų. Manytina, kad Lietuvoje elektroninės informacijos saugos reguliavimas įstatymo lygmeniu yra fragmentiškas ir nepakankamas[20].

JAV Federalinis informacijos saugos valdymo įstatymas specifines funkcijas informacijos saugos srityje numato federalinėms agentūroms, Nacionaliniam standartų ir technologijų institutui bei Valdymo ir biudžeto tarnybai (angl. *Office of Management and Budget*). Tuo tarpu Lietuvoje už elektroninės informacijos saugos priežiūrą, įgyvendinimą ir politikos formavimą atsakingos šios pagrindinės institucijos: Vidaus reikalų ministerija, Informacinės visuomenės plėtros komitetas, Ryšių reguliavimo tarnyba, Valstybinė duomenų apsaugos inspekcija ir Valstybės kontrolė.

JAV Federalinėms agentūroms informacijos saugos srityje suteikiama bei pavedama daug pareigų ir teisių informacijos saugos srityje. Federalinis informacijos saugos valdymo įstatymas iš kiekvienos agentūros vadovo reikalauja įgyvendinti atitinkamą informacijos saugos politiką, taip pat vykdyti veiksmus, efektyviai ir priimtinomis sąnaudomis mažinti informacijos saugos riziką, siekiant priimtinos rizikos lygio. Įstatymas taip pat reglamentuoja, jog kiekviena federalinė agentūra savo veikloje plėtotų ir įgyvendintų informacijos ir informacinių sistemų aprūpinimo informacijos sauga programą. Nacionalinis standartų ir technologijų institutas, atsakingas už standartus, gaires bei susijusias metodikas, turi užtikrinti adekvačią informacijos saugą federalinių agentūrų veikloje. Institutas glaudžiai bendradarbiauja su federalinėmis agentūromis, siekdamas gerinti įstatymo reikalavimų užtikrinti informacijos saugą supratimą bei įgyvendinimą, ir skelbia standartus bei gaires, kurios sudaro pagrindą tinkamoms informacijos saugos programoms šiose agentūrose.

Lietuvoje pagrindinės funkcijos elektroninės informacijos saugos srityje numatytos Vidaus reikalų ministerijai (formuoja valstybės politiką informacinių technologijų saugos srityje, organizuoja, koordinuoja ir kontroliuoja jos įgyvendinimą), Valstybinei duomenų apsaugos inspekcijai (plėtoja duomenų apsaugą, kontroliuoja asmens duomenų tvarkymo teisėtumą, kovoja su duomenų tvarkymo pažeidimais) ir Ryšių reguliavimo tarnybai (vykdo nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio CERT (*Computer Emergency Response Team*) veiklą, rengia elektroninės informacijos saugos grėsmių išvengimo rekomendacijas). Autorių nuomone, Lietuvoje trūksta vienos už informacijos saugą atsakingos institucijos, esamų institucijų funkcijos tam tikrais atvejais dubliuojasi, o viena iš pagrindinių institucijų – Lietuvos Respublikos vidaus reikalų ministerija – kontroliuoja kitas sau nepavaldžias ministerijas ir įstaigas ar institucijas (ydinga praktika).

JAV Federalinis informacijos saugos valdymo įstatymas įtvirtina, kad visos informacinės sistemos turi būti priskirtos tam tikroms kategorijoms, kurios nustatomos

20 Petrauskas, R.; Štitilis, D.; Rotomskis, I.; Paškauskas, Ž. International legislative Regulation Provisions Concerning the Security of Informations Systems and Information. Implementation of the Provisions in Lithuania. *Databases and Information Systems: seventh International baltic Conference on Databases and Information Systems.* Vilnius: Technika, 2006, p. 225.

pagal tikslus užtikrinti atitinkamą informacijos saugos lygį, atsižvelgiant į kylančios rizikos lygį. Saugos kategorijas nustato pirmasis privalomas įstatymo reikalaujamas saugos standartas – Federalinės informacijos ir informacinių sistemų priskyrimo saugos kategorijoms standartas[21]. Tuo tarpu Lietuvoje valstybės institucijų ir įstaigų informacinių sistemų klasifikavimą pagal informacinėse sistemose tvarkomos elektroninės informacijos svarbą reglamentuoja 2007 m. Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai[22].

Pažymėtina, kad tiek JAV federalinės informacinės sistemos, tiek Lietuvos viešojo sektoriaus informacinės sistemos turi atitikti įstatymų įgyvendinamųjų aktų – Minimalių federalinės informacijos ir informacinių sistemų saugos reikalavimų[23] (JAV) ir Vyriausybės 2007 m. balandžio 25 d. nutarimu Nr. 410 patvirtintų Bendrųjų elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimų[24] bei 2008 m. įsakymu Nr. 1V-384 patvirtintų Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos techninių saugos reikalavimų (Lietuvoje) – nustatytus saugos reikalavimus.

Už informacijos saugos reikalavimų nesilaikymą kyla atsakomybė. Pavyzdžiui, Lietuvoje Administracinių teisės pažeidimų kodekso 214(15) straipsnis numato administracinę atsakomybę už neteisėtą valstybės informacinių sistemų duomenų tvarkymą, o Baudžiamojo kodekso XXX skyriuje numatyta baudžiamoji atsakomybė už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui[25]. Tuo tarpu JAV atsakomybė už elektroninės informacijos saugos pažeidimus daugiausia numatyta kaip atsakomybė už elektroninius nusikaltimus (neteisėta prieiga ir kt.).

Atlikus pagrindinių Lietuvos ir JAV teisės aktų, reglamentuojančių elektroninės informacijos saugą, analizę, darytina išvada, kad šiuo metu Lietuvoje yra fragmentiškas elektroninės informacijos saugos reguliavimas, t. y. nėra teisės aktų, kurie išsamiai ir sistemiškai reglamentuotų tinklų ir elektroninės informacijos saugumą, o galiojantys teisės aktai neužtikrina visapusiško ir nuoseklaus tinklų ir elektroninės informacijos saugumo visuomeninių santykių reglamentavimo, nesudaro sąlygų vartotojų pasitikėjimui informacine visuomene ir saugios informacinės visuomenės plėtrai. Nors abiejose lygina-

21 FIPS PUB 199 "Standards for Security Categorization of Federal Information and Information Systems" [interaktyvus]. 2004 [žiūrėta 2011-05-03]. < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

22 Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai. *Valstybės žinios.* 2007, Nr. 78-3160.

23 FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"[interaktyvus]. 2006 [žiūrėta 2011-05-03]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf >.

24 Vyriausybės 2007 m. balandžio 25 d. nutarimu Nr. 410 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios.* 2007, Nr. 49-1891.

25 Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios.* 2000, Nr. 89-2741; XXX skyrius „Nusikaltimai elektroninių duomenų ir informacinių sistemų saugumui".

mose valstybėse galioja daug teisės aktų, reglamentuojančių elektroninės informacijos saugos klausimus viešajame sektoriuje, elektroninės informacijos sauga privačiame sektoriuje nėra reguliuojama[26], išskyrus tam tikras išimtis. Toks teisinis reguliavimas kritikuotinas, kadangi elektroninės informacijos sauga negali būti veiksmingai užtikrinama reguliuojant tik viešąjį sektorių, o privatųjį sektorių paliekant savireguliacijai. Taip pat atkreiptinas dėmesys, kad Lietuvoje trūksta vieningos elektroninės informacijos saugos institucinės kontrolės.

Neužtikrinus veiksmingo elektroninės informacijos saugos reguliavimo, sudaromos prielaidos tapatybės vagystei elektroninėje erdvėje.

3. Asmens identifikavimo teisinis reguliavimas

JAV teisinį tapatybės turinio elementų reguliavimą užtikrina savarankiškai, tuo tarpu Lietuva, būdama Europos Sąjungos valstybė narė, turi užtikrinti nacionalinių teisės aktų atitiktį Europos Sąjungos keliamiems reikalavimams.

Pagrindiniai asmens tapatybės dokumentai JAV yra pasas, paso kortelė ir socialinio draudimo pažymėjimas, Lietuvoje – pasas ir asmens tapatybės kortelė. Minėtų dokumentų išdavimas abiejose valstybėse yra centralizuotas, tačiau mažiau svarbių dokumentų išdavimo tvarka yra labai skirtinga: JAV yra federacinė valstybė ir valstijose šie dokumentai išduodami vadovaujantis skirtingą tvarką nustatančiais teisės aktais. Be to, JAV ypatumas asmens identifikavimo teisinio reguliavimo srityje, palyginti su Lietuva, yra tas, kad JAV nenaudoja oficialių, privalomų, įvairios paskirties identifikavimo kortelių, kartu – asmens kodų, kaip jie suprantami Lietuvoje: vietoj vieno kodo, naudojamo nusakant asmens tapatybę bet kurioje situacijoje, naudojami įvairūs siaurai taikomi žymenys.

Pasakytina, kad JAV vairuotojų pažymėjimus išduoda valstijos, o atsižvelgiant į tai, kad šioje valstybėje nėra nacionalinės identifikavimo kortelės, vairuotojo pažymėjimas paprastai naudojamas kaip tapatybės nustatymo formos standartas. Asmenims, kurie neturi vairuotojo pažymėjimo, valstijos išduoda identifikavimo korteles, tačiau jos nėra privalomos. Lietuvoje, skirtingai nei JAV, asmens tapatybės kortelė yra vienas iš pagrindinių asmens tapatybę patvirtinančių dokumentų, tačiau naujo pavyzdžio vairuotojo pažymėjimas Lietuvoje taip pat, kaip ir JAV, praktiškai naudojamas kaip tapatybės nustatymo dokumentas, nors teisės aktuose jis nėra įvardijamas kaip asmens tapatybę patvirtinantis dokumentas. Peržvelgus Lietuvoje veikiančių finansinių institucijų paslaugų teikimo sutartis, nustatyta, kad, pavyzdžiui, visi komerciniai bankai Lietuvoje kaip tapatybę patvirtinantį dokumentą pripažįsta ir vairuotojo pažymėjimą, išduotą po 2002 m. gruodžio 31 d. (naujo pavyzdžio).

Elektroninės tapatybės reguliavimo srityje JAV paminėtinas Elektroninių parašų globalioje ir nacionalinėje komercijoje aktas[27], kuris nustato elektroninio sertifikato tei-

---

26 Išskyrus (Lietuvoje) kelis fragmentinius teisės aktus – Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymą (dėl asmens duomenų saugumo), Lietuvos Respublikos elektroninių ryšių įstatymą (dėl elektroninių ryšių saugumo) ir kt.

27 Electronic signatures in global and national commerce act [interaktyvus]. [žiūrėta 2011 05 02]. <http://www.ftc.gov/os/2001/06/esign7.htm>.

sinę galią. Šiame įstatyme nurodoma, kad viena iš elektroninio parašo funkcijų yra pasirašančio asmens identifikavimas. JAV didžioji dalis elektroninių paslaugų sistemų naudoja panašias asmens identifikavimo priemones. Galima nurodyti svarbiausius asmens elektroninėje erdvėje identifikavimo elementus ir identifikavimo pavyzdžius JAV:[28]

1) identifikavimas pagal tai, ką vartotojas turi žinoti: asmuo elektroninėje erdvėje gali būti identifikuojamas pagal unikalų pavadinimą (vardą) ir slaptažodį. Fizinėje erdvėje asmenų vardai gali kartotis, tačiau toje pačioje elektroninėje sistemoje asmens tapatybė turi būti nustatoma naudojant unikalų identifikatorių;
2) identifikavimas pagal tai, ką vartotojas turi: šiuo principu grindžiamas kliento atpažinimas pagal turimas priemones: elektroninis parašas (patvirtintas elektroniniu sertifikatu), kodų generatoriai, kodų lentelės;
3) identifikavimas pagal tai, kas vartotojas yra: šiuo atveju panaudojami biometriniai tapatybės elementai, kurie leidžia identifikuoti asmenį pagal asmens specifines fiziologines arba elgesio charakteristikas.

Lietuvoje svarbiausi asmens identifikavimo elektroninėje erdvėje elementai ir identifikavimo pavyzdžiai analogiški JAV. Abiejose valstybėse įstatymiškai pripažįstamas ir reguliuojamas asmens identifikavimo būdas elektroninėje erdvėje – elektroninis parašas, patvirtintas elektroniniu sertifikatu. Lietuvoje elektroninį parašą ir elektroninį sertifikatą, kaip asmens tapatybės patvirtinimo būdą elektroninėje erdvėje, reguliuoja Elektroninio pašašo ir Asmens tapatybės kortelės įstatymai.

Paminėtina ir tai, kad abiejose lyginamose valstybėse elektroninės bankininkystės paslaugos naudoja savo identifikavimo sistemą, kuri apima du identifikavimo elektroninėje erdvėje elementus: „Tai ką žino“ ir „Tai ką turi“, ir kurią pripažįsta valstybė. Pavyzdžiui, Lietuvoje tokia elektroninė tapatybė remiasi Elektroninio parašo įstatymo 8 straipsnio 3 dalies nuostata: „Elektroninis parašas visais atvejais turi šio straipsnio 1 dalyje įtvirtintą teisinę galią, jeigu parašų naudotojai tarpusavyje dėl to susitaria“[29] ir ši tapatybė turi įstatymo teisinę galią. Banko ir kliento susitarimas, kad atitinkama banko sistema atitinka saugios sistemos požymius, minima įstatymo teises norma bei identifikavimas remiantis šia sistema ir suponuoja tą faktą, jog tokia identifikavimo sistema yra pripažįstama valstybės.

Atlikus pagrindinių JAV ir Lietuvos teisės aktų, reglamentuojančių asmens identifikavimą, analizę galima daryti išvadą, kad elektroninėje erdvėje elektroninis parašas (patvirtintas kvalifikuotu sertifikatu) (valstybės sureguliuota saugi identifikavimo priemonė) arba asmens identifikavimas naudojant bankines sistemas (valstybės pripažįstama tapatybė[30]) atitinka valstybės reguliuojamus tapatybės nustatymo būdus fizinėje erdvėje (kai tapatybė nustatoma dokumentų pagrindu).

---

28 Burr, W. E.; Dodson, D. F.; Polk, W. T. Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology [interaktyvus]. *Gaithersburg: NIST Special Publication* 800-63 Version 1.0.2., 2006 [žiūrėta 2011 05 02]. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.

29 Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios.* 2000, Nr. 61-1827.

30 Jei naudojamasi sutartiniu elektroniniu parašu.

Atlikta asmens tapatybės dokumentų teisinio reguliavimo analizė rodo, kad asmens dokumentų įvairovė JAV yra labai didelė, palyginti su asmens dokumentais, išduodamais Lietuvoje, o asmens identifikavimo dokumentų išdavimo tvarka JAV yra pakankamai lanksti. Taip pat atkreiptinas dėmesys, kad JAV padaroma daug nusikaltimų (tiek fizinėje erdvėje, tiek ir elektroninėje), kuriems padaryti neretai pasisavinami tapatybės duomenys. JAV didelis dėmesys yra skiriamas terorizmo prevencijai, todėl šioje valstybėje būtina užtikrinti minimalius asmens dokumentų apsaugos reikalavimus. Tam, kad būtų įvykdyti minimalūs dokumentams keliami reikalavimai, JAV valstijos, išduodamos asmens tapatybės korteles ir vairuotojo pažymėjimus, turi užtikrinti tinkamą dokumentų apsaugos lygį bei fiksuoti būtiną informaciją[31], priešingu atveju sudaromos prielaidos įvykdyti tapatybės vagystę.

4. Specialūs teisės aktai dėl tapatybės vagystės elektroninėje erdvėje

4.1. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas (baudžiamųjų įstatymų normos)

Tapatybės vagystės elektroninėje erdvėje sudėtingumas lemia nevienodą praktiką vertinant šią pavojingą veiką[32]. Vis dažniau kyla diskusijos dėl baudžiamosios atsakomybės. Pavyzdžiui, Ekonominio bendradarbiavimo ir plėtros organizacija[33] laikosi nuomonės, kad tapatybės vagystę reikia kriminalizuoti kaip savarankišką nusikalstamą veiką. Todėl svarbu palyginti JAV ir Lietuvos atitinkamas baudžiamųjų įstatymų normas.

Baudžiamųjų kodeksų normų, susijusių su tapatybės vagyste elektroninėje erdvėje, palyginimą tikslinga atlikti vadovaujantis tapatybės vagystės elektroninėje erdvėje stadijomis. Mokslinėje literatūroje dažniausiai skiriamos trys tapatybės vagystės stadijos: 1 stadija – su tapatybe susijusios informacijos gavimas, 2 stadija – sąveika su tapatybe susijusia informacija, 3 stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą[34].

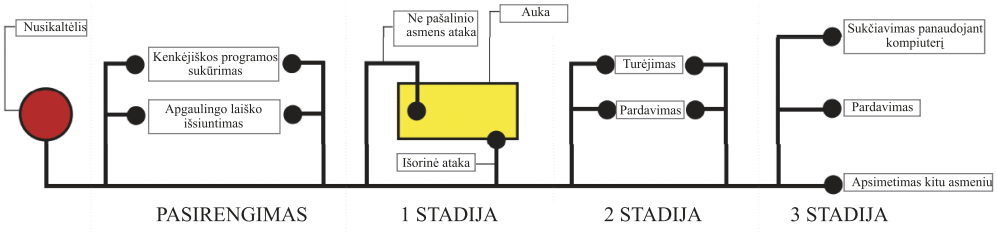
---

31 Division a emergency supplemental appropriations act for defense, the global war on terror, and tsunami relief. Sec. 202. Minimum document requirements and issuance standards for federal recognition [interaktyvus]. 2005 [žiūrėta 2011-05-02]. <http://www.dsca.mil/programs/LPA/2005/getdoc.cgi_dbname=109_cong_public_laws&docid=f_publ013.109.pdf>.

32 Štitilis, D.; Laurinaitis M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, Nr. 50: 244.

33 <http://www.oecd.org>.

34 Gercke, M. Internet-related identity thef. Project on Cybercrime [Interaktyvus]. 2007, p. 17-20. [žiūrėta 2011-05-06] <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.



Šaltinis: Gercke Marco. Internet-related identity thef. Project on Cybercrime, 2007[35]

1 pav. Tapatybės vagystės trijų stadijų modelis

JAV pagal nusikaltėlių, veikiančių elektroninėje erdvėje, skaičių užima antrą vietą pasaulyje[36]. Ši valstybė turi didžiulę patirtį kovojant su elektroniniais nusikaltimais, yra viena iš Konvencijos dėl elektroninių nusikaltimų[37] iniciatorių (Konvenciją ratifikavo 2006 m. rugsėjo 29 d., šalyje ji įsigaliojo nuo 2007 m. sausio 1 d.) ir ėmėsi daugybės priemonių, siekdama užkirsti kelią tapatybės nusikaltimams. Lietuva, kaip ir JAV, yra Konvencijos narė (Konvenciją ratifikavo 2004 m. kovo 18 d., ji šalyje įsigaliojo nuo 2004 m. liepos 1 d.), tačiau nors tapatybės vagystės elektroninėje erdvėje atvejų Lietuvoje pasitaiko vis daugiau, ši veika Lietuvoje nėra tokio didelio pavojingumo ir masto problema, kaip JAV. Lietuvos patirtis kovojant su tapatybės vagyste elektroninėje erdvėje, palyginti su JAV, yra menkesnė, o teisės aktuose vis dar yra spragų, sudarančių prielaidas atlikti šią pavojingą veiką.

Atkreiptinas dėmesys, kad JAV baudžiamosios teisės sistema yra labai sudėtinga, kadangi tuos pačius baudžiamosios teisės klausimus reguliuoja ir federalinė, ir valstijų baudžiamoji teisė, o federalinio baudžiamojo kodekso nėra. 1948 m. Kongreso įstatymu pirmą kartą buvo kodifikuoti visi federaliniai įstatymai. Įstatymai, reglamentuojantys baudžiamosios teisės santykius, buvo įtraukti į JAV įstatymų sąvado 18 **s**kirsnį „Nusikaltimai ir baudžiamasis procesas“.

Atlikus JAV įstatymų sąvado baudžiamosios teisės normų, reglamentuojančių atskirų nusikalstamų veikų sudėtis, analizę galima daryti išvadą, kad visos trys tapatybės vagystės stadijos – su tapatybe susijusios informacijos gavimas, tokios informacijos turėjimas ir panaudojimas siekiant padaryti nusikaltimą – yra kriminalizuotos. 1 stadija patenka į JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1030 straipsnio, reglamentuojančio sukčiavimą, naudojant kompiuterį, veikimo sritį, 2 stadija patenka

35 Gercke, M. Internet-related identity thef. *Project on Cybercrime* [interaktyvus], 2007, p. 17-20. [žiūrėta 2011-05-05]. <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.

36 Review 2005 of the Data Protection Ombudsman [interaktyvus]. [žiūrėta 2011-05-02]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.

37 Convention on Cybercrime [interaktyvus]. Budapest, 2001 [žiūrėta 2011-05-02]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

į 1002 straipsnio (suklastotų dokumentų turėjimas) bei 1028 straipsnio, numatančio baudžiamąją atsakomybę už sukčiavimą, susijusį su tapatybės nustatymo dokumentais, autentifikavimo priemonėmis ir informacija (perdavimas, turėjimas, prekyba) veikimo sritį, o 3 tapatybės vagystės stadija kriminalizuota minėtame 1028 straipsnyje (neteisėtas dokumentų, autentifikavimo priemonių ir informacijos gaminimas, klastojimas) bei 1037 straipsnyje, kuriame numatoma baudžiamoji atsakomybė už sukčiavimą naudojant elektroninį paštą[38].

Pažymėtina, jog 2 ir 3 tapatybės vagystės stadijos kriminalizuotos 1028 straipsnio (a) dalies (7) punkte, įtvirtinančiame tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtį. Taigi, 1998 m. JAV tapatybės vagystė buvo kriminalizuota kaip savarankiška veika: Kongresas Tapatybės vagystės ir apsimetinėjimo atgrasymo akte[39] (angl. *Identity Theft and Assumption Deterrence Act*) įtvirtino specifinės nusikalstamos veikos sudėtį, kuri buvo įtvirtinta JAV įstatymų sąvado 18 skirsnio 1 dalies 47 skyriaus 1028 straipsnio (a) dalies (7) punkte. Baudžiamoji atsakomybė numatyta už tai, kai kas nors tyčia perduoda, laiko, naudoja, neturėdamas tam teisės, kito asmens identifikavimo priemones, turėdamas tikslą padaryti arba tam, kad padarytų bet kokią neteisėtą veiką, kuri būtų Federacijos teisės pažeidimas arba kuri būtų sunkus nusikaltimas pagal galiojančius Valstijos ar vietinius teisės aktus[40]. Bausmė, numatoma už tokį nusikaltimą, yra laisvės atėmimas iki penkerių metų, o jei nusikaltimas padarytas sunkinančiomis aplinkybėmis[41] – laisvės atėmimas iki 15 metų.

Tuo tarpu atlikus Lietuvos Respublikos baudžiamojo kodekso teisės normų sisteminę analizę[42] nustatyta, kad tapatybės vagystės, kaip savarankiškos nusikalstamos veikos, sudėtis nėra įtvirtinta. Tam tikri tapatybės vagystės elektroninėje erdvėje elementai gali būti vertinami kaip pavojingos veikos, tačiau tapatybės vagystės elektroninėje erdvėje atvejais susiduriama su nusikalstamų veikų daugeto problema. 1 tapatybės vagystės stadiją – su tapatybe susijusios informacijos gavimą – kriminalizuoja Lietuvos Respublikos baudžiamojo kodekso 166, 167, 198, 198(1) ir 214 straipsniai. 3 tapatybės vagystės stadija – su tapatybe susijusios informacijos panaudojimas siekiant padaryti nusikaltimą – patenka į Lietuvos Respublikos 182, 207, 215 ir 300 straipsnius. Tapatybės vagystės 2 stadija (laikymas, perdavimas) iš dalies patenka į 198 ir 214 straipsnių veikimo sritį, tačiau tapatybės vagystės 2 stadijos elementas – su tapatybe susijusios informacijos turėjimas – Lietuvos Respublikos baudžiamajame kodekse nėra kriminalizuotas, o bau-

38 Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos*. 2011, 1 (3): 159.

39 Identity Theft and Assumption Deterrence Act [interaktyvus]. 1998 [žiūrėta 2011-05-02]. <http://www.ftc.gov/os/statutes/itada/itadact.htm>.

40 United States Code („U. S. C"), Title 18, Part I, Chapter 47, Section 1028 (a) (7) [interaktyvus]. [žiūrėta 2011-05-02]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

41 Sunkinančios aplinkybės numatytos 2004 m. Bausmės už tapatybės vagystę padidinimo akte (Identity Theft Enhancement Penalty Act) [interaktyvus]. [žiūrėta 2011-05-02]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

42 Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos*, 2011, 1 (3):165.

džiamąją atsakomybę užtraukia tik neviešų elektroninių duomenų ir svetimų, netikrų ar suklastotų elektroninių mokėjimo priemonių laikymas.

4.2. Kiti specialūs teisės aktai

Analizuojant teisės aktus, susijusius su tapatybės vagyste elektroninėje erdvėje, lyginamose valstybėse, nustatyta, kad Lietuvoje nėra specialiųjų teisės aktų dėl tapatybės vagystės elektroninėje erdvėje. Tuo tarpu JAV tokie teisės aktai egzistuoja, nepaisant to, kad tapatybės vagystė šioje valstybėje yra kriminalizuota. Dėl straipsnio ribotos apimties paminėtini šie pagrindiniai specialieji JAV teisės aktai tapatybės vagystės srityje:

– Sukčiavimo, susijusio su pašto paslaugomis, įstatymas (angl. *Mail Fraud Statute*[43]) (1872): skirtas apsaugoti visuomenę nuo bet kokios apgaulės ar sukčiavimo, įskaitant kreditinį sukčiavimą ir tapatybės vagystę. Sukčiavimas apibrėžiamas kaip bet koks bandymas suklaidinti ar gauti pinigų, įgyti kito turto, apgaulės būdu ar apsimetant kitu asmeniu. Pagal šį įstatymą baudžiamoji atsakomybė kyla tam, kas pavagia asmeninę informaciją, suklastoja prašymus gauti kreditinę kortelę ir paštu išsiunčia bankams ir kitoms kreditines korteles išduodančioms institucijoms. Taip pat pagal šį įstatymą baudžiama ir už kitus su tapatybe susijusius nusikaltimus, kuriuose paštas yra būtinas sukčiavimo įgyvendinimo elementas. Už minėtą nusikaltimą baudžiama bauda arba laisvės atėmimu iki 20 metų, arba ir bauda, ir laisvės atėmimu, o jei nuo to nukenčia ir finansų institucija – bauda iki 1 000 000 dolerių arba laisvės atėmimu iki 30 metų, arba ir bauda ir laisvės atėmimu;

– Padirbtų prieigos įrenginių, kompiuterinio klastojimo ir piktnaudžiavimo įstatymas (angl. *Counterfeit Access Device and Computer Fraud and Abuse Act*[44]) (1984): tai pirmasis federalinis įstatymas, skirtas kompiuteriniam sukčiavimui ir piktnaudžiavimui. Iki 1984 m. nebuvo įstatymo, numatančio baudžiamąją atsakomybę už kompiuterinius nusikaltimus. Iš pradžių įstatymas numatė baudžiamąjį persekiojimą už tris nusikalstamas kompiuterines veikas, kurios padaromos naudojant kompiuterį: neteisėtą prieigą prie valstybės paslaptį sudarančios informacijos, susijusios su nacionaliniu saugumu ir užsienio santykiais; netinkamą prieigą prie finansinių institucijų saugomos finansinės informacijos; netinkamą prieigą prie vyriausybės kompiuteryje saugomos informacijos. Vystantis technologijoms, pastebėta, kad įstatymo veikimo sritis yra gana siaura, todėl buvo daromos įstatymo pataisos ir bėgant laikui įstatymas kriminalizavo 7 kompiuterinio piktnaudžiavimo būdus (1996 m.) ir numatė galimybę pareikšti civilinį ieškinį (1990) už kompiuterinį nusikaltimą. Šiuo metu baudžiamoji atsakomybė pagal minėtą įstatymą kyla už šnipinėjimą elektroninėje erdvėje, neteisėtą prieigą prie finansinės informacijos, veiksmus, susijusius su vyriausybės kompiuteryje esančių duomenų peržiūra, vagystę iš apsaugotų kompiuterių, žalos sukėlimą netinkamai perduodant duomenis,

43 Mail Fraud Statute, Title 18, United States Code, Section 1341 [interaktyvus]. [žiūrėta 2011-05-02] <http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_63.html>.

44 Codified in Fraud and Related Activity in Connection with Computers, Title 18, United States Code, Section 1030. [interaktyvus]. [žiūrėta 2011-05-03].<http://www.law.cornell.edu/uscode/18/1030.html>.

prekybą slaptažodžiais ir kt. Už minėto įstatymo nuostatų pažeidimą numatoma bauda ir laisvės atėmimas iki 10 metų, o maksimali bausmė – laisvės atėmimas iki 20 metų.

– Bausmės už tapatybės vagystę padidinimo aktas (angl. *Identity Theft Enhancement Penalty Act*[45]) (2004): padidino laisvės atėmimo bausmę už tapatybės vagystę, kai padaromas kitas nusikaltimas, t. y. kai tapatybės vagyste pasinaudojama kaip priemone kitiems nusikaltimams, tokiems kaip terorizmas, nelegali imigracija, šaunamųjų ginklų kontrabanda, padaryti. Įstatymas numato, kad už tapatybės vagystę, padarytą sunkinančiomis aplinkybėmis, įprasta laisvės atėmimo bausmė už tapatybės vagystę prailginama dvejais metais, o jei tapatybės vagystė buvo padaryta tam, kad vėliau ja pasinaudojant būtų galima atlikti terorizmo veiksmus – laisvės atėmimo bausmė už tapatybės vagystę prailginama penkeriais metais.

– Teisingų ir tikslių kredito transakcijų aktas (angl. *Fair and Accurate Credit Transactions Act*[46]) (2003). Tai dar vienas federalinės vyriausybės bandymo apsaugoti elektroninę erdvę pavyzdys[47]. Šiuo įstatymu buvo patvirtintos tam tikros vartotojų apsaugos priemonės. Jis įtvirtina daug naujų kovos su tapatybės vagyste priemonių. Reikalaujama sukurti sukčiavimo pranešimo sistemą vartotojams, kurie galėjo tapti tapatybės vagystės aukomis, sutrumpinti kredito kortelės sąskaitos numerį, pateikiant elektroninius išrašus, sąskaitų blokavimą iš karto po to, kai vartojas užpildo pareiškimą policijoje, raudonų vėliavėlių indikatorių sukūrimą finansų institucijoms ir kreditoriams, pastebėjus tapatybės vagystę, ir kt. Įstatymas įtvirtina tokią tapatybės vagystės sąvoką: tapatybės vagystė – tai sukčiavimas, padarytas pasinaudojant kitą asmenį identifikuojančia informacija; taip pat nurodoma, kad tapatybės vagystė turėtų būti suprantama taip, kaip ją apibrėžia Komisija. Priimtas siekiant sumažinti tapatybės vagystės ir vartotojų apgaulių riziką. Įtvirtina reikalavimą, kad verslo subjektai, nepriklausomai nuo jų dydžio ir pramonės šakos, tinkamai saugotų ir disponuotų asmenine informacija, kurią jie renka apie savo vartotojus ir darbuotojus.

Atlikus JAV ir Lietuvos teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje, lyginamąją analizę, nustatyta, kad JAV, skirtingai nei Lietuvoje, ši pavojinga veika yra kriminalizuota ir už ją numatyta griežta baudžiamoji atsakomybė. Be to, JAV egzistuoja ir specialūs teisės aktai, nustatantys atsakomybę už tapatybės vagystę elektroninėje erdvėje. Toks JAV teisinis reguliavimas vertintinas kaip veiksminga kovos su tokio pobūdžio veikomis priemonė. Tuo tarpu Lietuvoje nėra specialių teisės aktų, reglamentuojančių tapatybės vagystę elektroninėje erdvėje, o Lietuvos Respublikos baudžiamojo kodekso normų analizė parodė, kad tapatybės vagystės elektroninėje erdvėje vertinimas baudžiamojoje teisėje gana sudėtingas, todėl Lietuvos Respublikos baudžiamajame kodekse būtų tikslinga įtvirtinti tapatybės vagystės elektroninėje erdvėje kaip savarankiškos nusikalstamos veikos sudėtį – tai leistų panaikinti tapatybės vagystės elektroninėje erdvėje teisinio reguliavimo spragas, palengvintų minėtos veikos įrodi-

45 Identity Theft Enhancement Penalty Act [interaktyvus]. [žiūrėta 2011-05-02]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

46 Fair and Accurate Credit Transactions Act [interaktyvus]. [žiūrėta 2011-05-02]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108>.

47 Ghosh S., Turrini E. Cybercrimes: A Multidisciplinary Analysis. *Springer-Verlag*, 2010; p. 247

nėjimą ir kvalifikavimą, be to, siekiant patraukti asmenį baudžiamojon atsakomybėn už tapatybės vagystę elektroninėje erdvėje, padėtų išvengti gana sudėtingo nusikalstamų veikų daugeto įrodinėjimo.

Išvados

1. Atitinkamų teisės aktų asmens duomenų teisinės apsaugos srityje lyginamoji analizė parodė, jog Lietuvoje asmens duomenų teisinis reguliavimas yra pakankamas, išskyrus sankcijas už asmens duomenų teisinės apsaugos reikalaivmų pažeidimus. Jos turėtų būti peržiūrėtos ir sugriežtintos.

2. Elektroninių duomenų saugumo teisinio reguliavimo lyginamose valstybėse analizė atsleidė, kad Lietuvoje trūksta holistinio požiūrio reglamentuojant elektroninės informacijos saugą (įskaitant ir institucinės kontrolės aspektą). Abiejose valstybėse elektroninės informacijos sauga turėtų būti reguliuojama ir privačiame sektoriuje. Šie elektroninės informacijos saugos teisinio reguliavimo trūkumai sudaro prielaidas tapatybės vagystės elektroninėje erdvėje paplitimui.

3. Atlikus asmens tapatybės dokumentų teisinio reguliavimo analizę, nustatyta, kad asmens dokumentų įvairovė JAV, palyginti su asmens dokumentais, išduodamais Lietuvoje, yra labai didelė, o asmens identifikavimo dokumentų išdavimo tvarka JAV yra pakankamai lanksti. JAV padaroma daug nusikaltimų (tiek fizinėje erdvėje, tiek ir elektroninėje), kuriems atlikti neretai pasisavinami tapatybės duomenys. Be to, JAV didelis dėmesys skiriamas terorizmo prevencijai, todėl šioje valstybėje būtina užtikrinti minimalius asmens dokumentų apsaugos reikalavimus. Tam, kad būtų įvykdyti minimalūs dokumentams keliami reikalavimai, JAV valstijos, išduodamos asmens tapatybės korteles ir vairuotojo pažymėjimus, turi užtikrinti tinkamą dokumentų apsaugos lygį bei fiksuoti būtiną informaciją, priešingu atveju sudaromos prielaidos tapatybės vagystei.

4. Specialių teisės aktų, susijusių su tapatybės vagyste elektroninėje erdvėje, lyginamoji analizė parodė, jog JAV yra ne vienas specialus teisės aktas, susijęs su tapatybės vagyste elektroninėje erdvėje (tai pagerina kovą su šiuo socialiniu-teisiniu reiškiniu), tuo tarpu Lietuvoje nėra nė vieno specialaus teisės akto, kuris reglamentuotų minimus santykius, ir tai, autorių nuomone, sudaro palankias sąlygas plisti tapatybės vagystės elektroninėje erdvėje reiškiniui Lietuvoje.

5. Baudžiamųjų normų lyginamoji analizė parodė, jog JAV tapatybės vagystė elektroninėje erdvėje kriminalizuota kaip savarankiška veika. Tai turėtų gerinti tokios veikos tyrimą, tuo tarpu Lietuvoje už tam tikrus tapatybės vagystės elektroninėje erdvėje elementus baudžiamoji atsakomybė galima tik pagal tradicines pavojingas veikas (sukčiavimas ir pan.), dėl ko tokią veikią įrodyti yra daug sunkiau.

6. Tiek Lietuvoje, tiek JAV identifikuotas teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, trūkumas. Tai trukdo sėkmingai kovoti su šiuo pavojingu socialiniu-teisiniu reiškiniu.

7. Nustatyti šie teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, trūkumai Lietuvoje: specialių teisės aktų, skirtų tapatybės vagystei elektroninėje

erdvėje, srityje bei nustatant baudžiamąją atsakomybę už tapatybės vagystę elektroninėje erdvėje (tapatybės vagystę elektroninėje erdvėje įvardijant kaip savarankišką pavojingą veiką). Lietuvos įstatymų leidėjas, numatydamas pagrindines teisinio reguliavimo, susijusio su tapatybės vagyste elektroninėje erdvėje, tobulinimo sritis, turėtų atsižvelgti į tyrimo identifikuotas problemas.

Literatūa

„Saugaus uosto“ principai [interaktyvus]. [žiūrėta 2011-05-03]. <https://www.export.gov/safeharbor/eu/eg_main_018476.asp>.

Vyriausybės 2007 m. balandžio 25 d. nutarimu Nr. 410 patvirtinti Bendrieji elektroninės informacijos saugos valstybės institucijų ir įstaigų informacinėse sistemose reikalavimai. *Valstybės žinios.* 2007, Nr. 49-1891.

Burr, W. E.; Dodson, D. F.; Polk, W. T. Electronic Authentication Guideline. Recommendations of the National Institute of Standards and Technology [interaktyvus]. *Gaithersburg: NIST Special Publication* 800-63 Version 1.0.2., 2006 [žiūrėta 2011 05 02]. <http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>.

Civilka, M. Asmens duomenų apsaugos teisinis reguliavimas interneto kontekste [interaktyvus]. [žiūrėta 2011-05-03]. <http://www.google.lt/url?q=http://ututi.lt/subject/VU/EF/elektroninis_verslas/file/3412/get&sa=U&ei=CIrBTYT rGcqYOsXO7Z0I&ved=0CAsQFjAA&usg=AFQjCNGhewAzJu8FWWwu2xDHpalcdnv-sg>.

Codified in Fraud and Related Activity in Connection with Computers, Title 18, United States Code, Section 1030 [interaktyvus]. [žiūrėta 2011-05-03]. <http://www.law.cornell.edu/uscode/18/1030.html>.

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (entered into force on 1 October 1985) [interaktyvus]. CETS 108 [žiūrėta 2011-05-03]. <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=8&DF=26/04/2011&CL=ENG>.

Convention on Cybercrime [interaktyvus]. Budapest, 2001 [žiūrėta 2011-05-02]. <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

Division a emergency supplemental appropriations act for defense, the global war on terror, and tsunami relief. Sec. 202. Minimum document requirements and issuance standards for federal recognition [interaktyvus]. 2005 [žiūrėta 2011-05-02]. <http://www.dsca.mil/programs/LPA/2005/getdoc.cgi_dbname=109_cong_public_laws&docid=f_publ013.109.pdf>.

Electronic signatures in global and national commerce act [interaktyvus]. [žiūrėta 2011 05 02]. <http://www.ftc.gov/os/2001/06/esign7.htm>.

Europos Parlamento ir Tarybos 1995 m. spalio 24 d. direktyva 95/46/EB dėl asmenų apsaugos tvarkant asmens duomenis ir laisvo tokių duomenų judėjimo [interaktyvus]. [1995] OL L281/31 [žiūrėta 2011-05-03]. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1995L0046:20031120:LT:PDF> .

Fair and Accurate Credit Transactions Act [interaktyvus]. [žiūrėta 2011-05-02]. <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108>.

False Statements Act (18 U.S.C. § 1001) [interaktyvus]. [žiūrėta 2011-05-03]. <http://www.law.cornell.edu/uscode/18/usc_sec_18_00001001----000-.html>.

Federal Information Security Management Act, 2002. US code, Title 44, Chapter 35, Subchapter III [interaktyvus]. [žiūrėta 2011-

05-03]. <http://www.law.cornell.edu/uscode/44/usc_sup_01_44_10_35_20_III.html>.

FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems" [interaktyvus]. 2006 [žiūrėta 2011-05-03]. <http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf >.

FIPS PUB 199 "Standards for Security Categorization of Federal Information and Information Systems" [interaktyvus]. 2004 [žiūrėta 2011-05-03]. < http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

Gercke, M. Internet-related identity thef. Project on Cybercrime [interaktyvus]. 2007 [žiūrėta 2011-05-05]. <http://www.coe.int/T/DG1/LegalCooperation/Economiccrime/cybercrime/cy%20activity_events_on_identity_theft/567%20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf>.

Ghosh S., Turrini E. Cybercrimes: A Multidisciplinary Analysis. Springer-Verlag, 2010

Higgins E. G. Cybercrime: An Introduction to an Emerging Phenomen. McGraw-Hill, 2010

Identity Theft and Assumption Deterrence Act [interaktyvus]. 1998 [žiūrėta 2011-05-02]. <http://www.ftc.gov/os/statutes/itada/itadact.htm>.

Identity Theft Enhancement Penalty Act [interaktyvus]. [žiūrėta 2011-05-02] <http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ275.108.pdf>.

Kiškis, M., *et al*. *Teisės informatika ir informatikos teisė*. Vilnius: Mykolo Romerio universiteto Leidybos centras, 2006. – 256 p.

Komisijos 2000 m. liepos 26 d. sprendimas dėl Europos Parlamento ir Tarybos direktyvos 95/46/EB dėl „saugaus uosto" privatumo principų teikiamos apsaugos pakankamumo ir su tuo susijusių JAV komercijos departamento pateiktų „Dažnai užduodamų klausimų". [2000] OL L 215.

Konvencija dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu. *Valstybės žinios*. 2001, Nr. 32-1059.

Kuner, C. European Data Privacy law and Online Business. *Oxford: Oxford University Press*, 2003.

Lietuvos Respublikos administracinių teisės pažeidimų kodeksas. *Valstybės žinios*. 1985, Nr. 1-1.

Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas. *Valstybės žinios.* 1996, Nr. 63-1479; 2003, Nr. 15-597; 2008, Nr. 22-804.

Lietuvos Respublikos baudžiamasis kodeksas. *Valstybės žinios.* 2000, Nr. 89-2741.

Lietuvos Respublikos elektroninio parašo įstatymas. *Valstybės žinios.* 2000, Nr. 61-1827.

Lietuvos Respublikos vidaus reikalų ministro įsakymu Nr. 1V-247 patvirtintos Valstybės institucijų ir įstaigų informacinių sistemų klasifikavimo pagal jose tvarkomą elektroninę informaciją gairės ir Valstybės institucijų ir įstaigų informacinių sistemų elektroninės informacijos saugos reikalavimai. *Valstybės žinios.* 2007, Nr. 78-3160.

Mail Fraud Statute, Title 18, United States Code, Section 1341. [interaktyvus]. [žiūrėta 2011-05-02]. <http://www.law.cornell.edu/uscode/18/usc_sup_01_18_10_I_20_63.html>.

Petrauskas, R.; Štitilis, D.; Rotomskis, I.; Paškauskas, Ž. International legislative Regulation Provisions Concerning the Security of Informations Systems and Information. Implementation of the Provisions in Lithuania. *Databases and Information Systems: seventh International baltic Conference on Databases and Information Systems.* Vilnius: Technika, 2006.

Review 2005 of the Data Protection Ombudsman [interaktyvus]. [žiūrėta 2011-05-02]. <www.tietosuoja.fi/uploads/q0vw1ft5.rtf>.

Štitilis, D.; Laurinaitis, M. Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai.* 2009, 50.

Štitilis, D.; Pakutinskas, P.; Dauparaitė, I.; Laurinaitis, M. Tapatybės vagystės elektroninėje erdvėje kriminalizavimas: lyginamieji aspektai. *Socialinių mokslų studijos*. 2011, 1 (3).

Štitilis, D.; Paškauskas, Ž. Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Jurisprudencija*. 2007, 92 (2).

United States Code („U. S. C"), Title 18, Part I, Chapter 47, Section 1028 (a) (7) [interaktyvus]. [žiūrėta 2011-05-02]. <http://www.law.cornell.edu/uscode/html/uscode18/usc_sec_18_00001028----000-.html>.

LEGAL ENVIRONMENT AGAINST ONLINE IDENTITY THEFT: COMPARATIVE ANALYSIS OF USA'S AND LITHUANIA'S LEGISLATION

Darius Štitilis, Paulius Pakutinskas, Inga Dauparaitė, Marius Laurinaitis

Mykolas Romeris University, Lithuania,. stitilis@mruni.eu

Summary. *The growth of the Internet and e-commerce has taken identity theft to new levels. Indeed, consumers, financial institutions and the whole economic suffer from online identity theft.*

This article analyses the legal environment which is concerned with online identity theft. The analysis is based on the comparison of two countries—USA's and Lithuania's—legislation, regulating such fields as personal data protection, electronic information security, identification, criminal liability and special legal acts, regulating online identity theft, because if all these fields are sufficiently regulated, the fight with online identity theft is more successful. The choice of the countries is based on the fact that USA has experience in fighting online identity theft while Lithuania is taken into a deeper consideration as it is a member of the European Union, the legal system of which has great differences in comparison to the USA.

The analysis of legislation, regulating personal data protection, is based on comparison of the main requirements and principles of personal data protection, institutions which are responsible for personal data protection and liability for breaches of personal data protection rules. The authors of the present article also present similarities and differences of legal regulation of electronic information security in USA and Lithuania by comparing the institutional control of information security, main requirements for information security and liability for breaches of information security rules. Also, the variety of personal identity documents in the USA and Lithuania is analyzed, main personal identity documents are presented as well as regulation of online identity theft, elements and types of identification online are discussed. Moreover, criminal and special legislation of USA and Lithuania is

taken into consideration in order to discuss and compare criminalization aspects of online identity theft.

In this article it is emphasized that although in USA online identity theft is criminalized, there also is special legislation concerned with online identity theft and this should be considered as an effective measure against online identity theft. Since in Lithuania the estimation of online identity theft from the point of criminal law is quite complicated, it is suggested that online identity theft should be criminalized as well as it is criminalized in USA. In addition, the authors notice that electronic information security should be regulated in both—private and public sectors not only in the public sector as it is at the present time.

The research has also shown that in Lithuania legal regulation of personal data is sufficient, except the sanctions for breaches of the requirements of personal data protection. However, the lack of legal regulation concerned with online identity theft is noticed in Lithuania and such a legal environment leads to advantageous conditions to commit online identity theft.

***Keywords**: legal environment against online identity theft, data protection, information security, identification.*